Dialogic®

Dialogic® DSI Signaling Servers

SS7G41 Operators Manual

Copyright and Legal Notice

Copyright © 2012-2014 Dialogic Inc. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Inc. at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

Publication Date: October 2014

Document Number: 64-1186-11

Contents

1 Overview 14
- 1.1 Introduction 14
  - 1.1.1 Related Information 15
  - 1.1.2 Applicability 15
- 1.2 Capacity 16
  - 1.2.1 SS7G41 Common Capabilities 16
  - 1.2.2 SS7G41 Capacities - SIU Mode 17
  - 1.2.3 SS7G41 Capacities - SWS Mode 17

2 Licensing, Installation, and Initial Configuration 19
- 2.1 Software Licensing 19
  - 2.1.1 Purchasing Software Licenses 19
  - 2.1.2 Supported Licenses 20
  - 2.1.3 Cumulative Licensing 21
  - 2.1.4 Temporary Licenses 21
  - 2.1.5 Evaluation Mode 22
- 2.2 Installation 22
  - 2.2.1 Connecting a VT100 Terminal 22
  - 2.2.2 Connecting via Telnet 23
  - 2.2.3 Initial IP Configuration 24
  - 2.2.4 Software Download 25
  - 2.2.5 Updating System Software 25
  - 2.2.6 Installing Software Licenses 27
- 2.3 Configuration 28

3 Access Control and Security 29
- 3.1 Concepts 29
- 3.2 System Policy 29
- 3.3 Access Control 29
- 3.4 Access Rights 29
  - 3.4.1 User Account Management 30
  - 3.4.2 User Access Profiles 30
- 3.5 Security 31
  - 3.5.1 HTTP Access 31
  - 3.5.2 Firewall 31
  - 3.5.3 SSH 32
  - 3.5.4 Configuring Public-Key Authentication for SSH 32
  - 3.5.5 SSH Tunneling for RSI 33

4 System Management 35
- 4.1 Web Interface 35
  - 4.1.1 DSH Flow Management Menu 37
- 4.2 Diagnostics, Alarms, and Logs 39
- 4.3 Automatic MMI Logging 40
- 4.4 Alarm Listing 40
- 4.5 SIGTRAN Throughput Licensing 48
- 4.6 SNMP 49
  - 4.6.1 DSMI SNMP 49
- 4.7 Lights Out Management 49
  - 4.7.1 Using the Remote Management Interface 49
  - 4.7.2 Changing the IP Address of the Remote Management Interface 50
- 4.8 Hard Disk Management 51
  - 4.8.1 Hard Disk Drive RAID Management 51
- 4.9 System Backup and Restoration 52

5 Configuration Commands 55
5.1 Overview 55
5.1.1 Syntax Conventions 56
5.1.2 Dynamic Configuration 57
5.1.3 Programming Circuit Group Configuration 57
5.2 Command Sequence 57
5.3 Detection of Errors in the Configuration File 59
5.4 SIU Environment Commands 60
5.4.1 IP_TOKEN - IP Token Configuration 60
5.4.2 IP_HOST - IP Host Configuration 60
5.4.3 MULTI_NODE - Multi-Node Configuration 61
5.4.4 SIU_HOSTS - SIU Host Settings Configuration 62
5.4.5 SIU_DUAL - DUAL SIU Configuration 63
5.5 Physical Interface Commands 64
5.5.1 SS7_BOARD - SS7 Board Configuration 64
5.5.2 LIU_CONFIG - Line Interface Configuration 65
5.5.3 STREAM_XCON - Cross Connect Configuration 68
5.5.4 ATM_CELL_STREAM - ATM Cell Stream Configuration 69
5.6 MTP Commands 70
5.6.1 MTP_CONFIG - Global MTP Configuration 71
5.6.2 MTP_LINKSET - MTP Link Set 73
5.6.3 MTP_LINK - MTP Signaling Link 74
5.6.4 MTP_ROUTE - MTP Route 78
5.6.5 MTP2_TIMER - MTP2 Timer Configuration 80
5.6.6 MTP3_TIMER - MTP3 Timer Configuration 81
5.6.7 QSAAL_TIMER - QSAAL Timer Configuration 83
5.6.8 MTP_USER_PART - MTP User Part 84
5.6.9 MONITOR_LINK - Monitor Link 85
5.7 SIGTRAN Configuration Commands 89
5.7.1 STN_CONFIG - SIGTRAN Configuration 89
5.7.2 STN_LAS - SIGTRAN Local Application Server Configuration 90
5.7.3 STN_LINK - SIGTRAN Link Configuration 92
5.7.4 STN_RAS - SIGTRAN Remote Application Server Configuration 94
5.7.5 STN_RASLIST - SIGTRAN Remote Application Server List Configuration 96
5.7.6 STN_ROUTE - SIGTRAN Route Configuration 96
5.7.7 STN_RSGLIST - SIGTRAN Route Signaling Gateway List Configuration 98
5.7.8 STN_LBIND - SIGTRAN Local Bind Configuration 99
5.7.9 SCTP_TIMER - SCTP Timer Configuration 100
5.7.10 M2PA_TIMER - M2PA Timer Configuration 101
5.7.11 M3UA_TIMER - M3UA Timer Configuration 102
5.8 Message Router Configuration Commands 103
5.8.1 MRF_OG - Message Router Origin Configuration 103
5.8.2 MRF_DE - Message Router Destination Configuration 105
5.8.3 MRF_RK - Message Router Routing Key Configuration 106
5.8.4 MRF_CP - Message Router Custom Profile Configuration 108
5.8.5 MRF_CE - Message Router Concerned Entity 109
5.9 ISUP Configuration Commands 110
5.9.1 ISUP_CONFIG - ISUP Configuration 110
5.9.2 ISUP_CFG_CCTGRP - ISUP Circuit Group Configuration 111
5.9.3 ISUP_TIMER - ISUP Timer Configuration 114

5.10 SCCP Configuration Commands 115
5.10.1 SCCP_CONFIG - SCCP Configuration 116
5.10.2 SCCP_LOAD_SHARE_TABLE - SCCP Load Share Table 117
5.10.3 SCCP_LOAD_SHARE_DPC - SCCP Load Shared DPCs 118
5.10.4 SCCP_GTT - Global Title Translations 119
5.10.5 SCCP_GTT_ADDRESS - Global Title Translation Address 121
5.10.6 SCCP_GTT_PATTERN - Global Title Translation Pattern 123
5.10.7 SCCP_RSP - SCCP Remote Signaling Points 126
5.10.8 SCCP_LSS - SCCP Local Sub-Systems 127
5.10.9 SCCP_RSS - SCCP Remote Sub-Systems 129
5.10.10 SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration 130
5.11 DTS Configuration Commands 131
5.12 The DTS configuration commands include the following: 131
5.12.1 DTS_CONFIG - Distributed Transaction Server Configuration 131
5.12.2 DTS_ROUTE - Configuration DTS Route Initiate 132
5.13 TCAP Configuration Commands 133
5.13.1 TCAP_CONFIG - TCAP Configuration 133
5.13.2 TCAP_NC_CONFIG - TCAP Network Context Configuration 134
5.13.3 TCAP_CFG_DGRP - TCAP Dialog Group Configuration 135
5.13.4 TCAP_TIMER - TCAP Timer Configuration 136
5.14 MAP Configuration Commands 137
5.14.1 MAP_CONFIG - MAP Configuration 137
5.14.2 MAP_NC_CONFIG - MAP Configuration 138
5.15 IS41 Configuration Commands 138
5.16 INAP Configuration Commands 138
5.16.1 INAP_CONFIG - INAP Configuration 139
5.16.2 INAP_NC_CONFIG - INAP Network Context Configuration 139
5.16.3 INAP_FE - INAP Functional Entities 140
5.16.4 INAP_AC - INAP Application Context 141

6 Management Commands 143
6.1 Access Control Commands 143
6.1.1 ACCUP - Access Current User Configuration 143
6.1.2 ACCUS - Account Control Current User Set 144
6.1.3 ACPOP - Account Control Policy Configuration 144
6.1.4 ACPOS - Account Control Policy Set 145
6.1.5 ACUAC - Account Control User Account Change 145
6.1.6 ACUAE - Account Control User Account End 146
6.1.7 ACUAI - Account Control User Account Initiate 146
6.1.8 ACUAP - Account Control User Account Configuration 146
6.1.9 ACUPC - Account Control User Profile Change 147
6.1.10 ACUPE - Account Control User Profile End 147
6.1.11 ACUPI - Account Control User Profile Initiate 148
6.1.12 ACUPP - Account Control User Profile Configuration 148
6.2 Alarm Commands 149
6.2.1 ALCDP - Alarm Codes 149
6.2.2 ALLIP - Active Alarm List 151
6.2.3 ALLOP - Alarm Log 151
6.2.4 ALTEE - Alarm Test End 152
6.2.5 ALTEI - Alarm Test Initiate 152

6.3 Configuration Commands 153
6.3.1 CNACE - ATM Cell Stream End 156
6.3.2 CNACI - ATM Cell Stream Initiate 157
6.3.3 CNACP - ATM Cell Stream Configuration 158
6.3.4 CNBOP - Board Configuration 158
6.3.5 CNBOS - Board Set 159
6.3.6 CNCGE - Circuit Group End 159
6.3.7 CNCGI - Circuit Group Initiate 160
6.3.8 CNCGP - Circuit Group Configuration 161
6.3.9 CNCRE - SS7 Route End 161
6.3.10 CNCRI - SS7 Route Initiate 162
6.3.11 CNCRP - SS7 Route Configuration 163
6.3.12 CNCSE - SCCP Concerned Subsystem Resource End 163
6.3.13 CNCSI - SCCP Concerned Subsystem Resource Initiate 164
6.3.14 CNCSP - SCCP Concerned Subsystem Resource Configuration 165
6.3.15 CNDRE - DTS Host Route End 165
6.3.16 CNDRI - DTS Host Route Initiate 166
6.3.17 CNDRP - DTS Host Routing Resource Print 167
6.3.18 CNDUP - Dual Operation Configuration 167
6.3.19 CNGAE - SCCP GTT Address End 168
6.3.20 CNGAI - SCCP GTT Address Initiate 168
6.3.21 CNGAP - SCCP GTT Address Configuration 169
6.3.22 CNGLE - SIGTRAN Gateway List End 170
6.3.23 CNGLI - SIGTRAN Gateway List Initiate 170
6.3.24 CNGLP - SIGTRAN Remote Signaling Gateway List Configuration 171
6.3.25 CNGPE - SCCP GTT Pattern End 172
6.3.26 CNGPI - SCCP GTT Pattern Initiate 173
6.3.27 CNGPP - SCCP GTT Pattern Configuration 173
6.3.28 CNGTE - SCCP GTT Translation End 174
6.3.29 CNGTI - SCCP GTT Translation Initiate 174
6.3.30 CNGTP - SCCP GTT Translation Configuration 175
6.3.31 CNHSP - Host Configuration 176
6.3.32 CNLAE - SIGTRAN Local Application Server End 176
6.3.33 CNLAI - SIGTRAN Local Application Server Initiate 177
6.3.34 CNLAP - SIGTRAN Local Application Server Configuration 178
6.3.35 CNLCP - Software License Capability Configuration 178
6.3.36 CNLDE - SCCP Loadshare DPC Configuration End 179
6.3.37 CNLDI - SCCP Loadshare DPC Configuration 179
6.3.38 CNLDP - SCCP Loadshare DPC Configuration 180
6.3.39 CNLSE - SS7 Link Set End 181
6.3.40 CNLSI - SS7 Link Set Initiate 181
6.3.41 CNLSP - SS7 Link Set Configuration 182
6.3.42 CNLTE - SCCP Loadshare Table Configuration End 182
6.3.43 CNLTI - SCCP Loadshare Table Configuration 183
6.3.44 CNLTP - SCCP Loadshare Table Configuration 184
6.3.45 CNMLE - SS7 Monitor Link End 184
6.3.46 CNMLI - SS7 Monitor Link Initiate 185
6.3.47 CNMLP - SS7 Monitor link Configuration 186
6.3.48 CNMNI / CNMNE - Multi-Node Configuration 186
6.3.49 CNMNP - Multi-Node Configuration Print 187
6.3.50 CNOBP - SNMP Trap Configuration 187
6.3.51 CNOBS - Configuration SNMP Traps Set 188
6.3.52 CNPCE - PCM End 189
6.3.53 CNPCI - PCM Initiate 190
6.3.54 CNPCP - PCM Configuration 190

6.3.55 CNRAE - SIGTRAN Remote Application Server End 191
6.3.56 CNRAI - SIGTRAN Remote Application Server Initiate 192
6.3.57 CNRAP - SIGTRAN Remote Application Server Configuration 192
6.3.58 CNRDI - Configuration Restore Default Initiate 193
6.3.59 CNRLE - SIGTRAN Remote Application Server List End 193
6.3.60 CNRLI - SIGTRAN Remote Application Server List Initiate 194
6.3.61 CNRLP - SIGTRAN Remote Application Server List Configuration 195
6.3.62 CNSBE - SIGTRAN Local Bind End 195
6.3.63 CNSBI - SIGTRAN Local Bind Initiate 196
6.3.64 CNSBP - SIGTRAN Local Bind Configuration 197
6.3.65 CNSLE - SS7 Link End 197
6.3.66 CNSLI - SS7 Link Initiate 198
6.3.67 CNSLP - SS7 Link Configuration 199
6.3.68 CNSMC - Configuration SNMP Manager Change 199
6.3.69 CNSME - Configuration SNMP Manager End 200
6.3.70 CNSMI - Configuration SNMP Manager Initiate 200
6.3.71 CNSMP - SNMP Manager Configuration 202
6.3.72 CNSNP - SNMP Configuration 202
6.3.73 CNSNS - Configuration SNMP Set 203
6.3.74 CNSRE - SIGTRAN Route End 203
6.3.75 CNSRI - SIGTRAN Route Initiate 204
6.3.76 CNSRP - SIGTRAN Route Configuration 205
6.3.77 CNSSE - SCCP Subsystem Resource End 205
6.3.78 CNSSI - SCCP Subsystem Resource Initiate 206
6.3.79 CNSSP - SCCP Subsystem Resource Configuration 207
6.3.80 CNSTE - SIGTRAN Link End 207
6.3.81 CNSTI - SIGTRAN Link Initiate 208
6.3.82 CNSTP - SIGTRAN Link Configuration 208
6.3.83 CNSWP - System Software Configuration 209
6.3.84 CNSYP - System Configuration 210
6.3.85 CNSYS - Configuration System Set 210
6.3.86 CNTDP - Time and Date Configuration 211
6.3.87 CNTDS - Configuration Time and Day Set 211
6.3.88 CNTMP - Trace Masks Configuration 212
6.3.89 CNTMS - Configuration Trace Mask Set 212
6.3.90 CNTPE - Configuration Network Time Protocol Server End 213
6.3.91 CNTPI - Configuration Network Time Protocol Server Initiate 214
6.3.92 CNTPP - NTP Server Configuration 214
6.3.93 CNURC - Configuration Update Resources Change 215
6.3.94 CNURE - Configuration Update Resources End 215
6.3.95 CNURI - Configuration Update Resources Initiate 216
6.3.96 CNUSC - Configuration SNMP User Change 216
6.3.97 CNUSE - Configuration SNMP User End 217
6.3.98 CNUSI - Configuration SNMP User Initiate 217
6.3.99 CNUSP - SNMP User Configuration 218
6.4 Database Commands 218
6.4.1 DBSVP - Subscriber Database Service Configuration 219
6.4.2 DBSVS – Subscriber Database Service Change 219
6.5 Helix Commands 220
6.5.1 HDPRP - Diameter Peer Configuration 221
6.5.2 HMFES - Flow Environment Configuration 221
6.5.3 HMFEP - Flow Environment Configuration 222

6.6 IP Commands 222
6.6.1 IPFWC - IP Firewall Change 223
6.6.2 IPFWE - IP Firewall End 223
6.6.3 IPFWI - IP Firewall Initiate 224
6.6.4 IPFWP - IP Firewall Configuration 224
6.6.5 IPGWE - IP Gateway End 225
6.6.6 IPGWI - IP Gateway Initiate 225
6.6.7 IPGWP - IP Gateway Configuration 226
6.6.8 IPLGE - IP Log End 226
6.6.9 IPLGI - IP Log Initiate 227
6.6.10 IPLGP - IP Log Configuration 227
6.6.11 IPNIC - IP Network Interface Configuration Change 228
6.6.12 IPNIE - IP Network Interface Configuration End 229
6.6.13 IPNII - IP Network Interface Configuration 229
6.6.14 IPNIP - Network Interface Configuration 230
6.6.15 IPHNTKE - IP Host NameToken Configuration End 230
6.6.16 IPHNIPTKI - IP Host NameToken Configuration 231
6.6.17 IPHNIPTKP - IP Host NameToken Configuration 231
6.6.18 IPWSP - IP Web Server Configuration 232
6.6.19 IPWSS - Configuration Web Service Set 232
6.7 MAP Services Commands 233
6.7.1 MAHRI / MAHRC / MAHRE - MAP HLR Rx Profile 234
6.7.2 MAHRP - MAP HLR Rx Profile Print 234
6.7.3 MAHTI / MAHTC / MAHTE - MAP HLR Tx Profile 235
6.7.4 MAHTP - MAP HLR Tx Profile Print 236
6.7.5 MAORI / MAORC / MAORE- MAP MO-SMS Rx Profile 237
6.7.6 MAORP - MAP MO-SMS Rx Profile Print 237
6.7.7 MAOTI / MAOTC / MAOTE - MAP MO-SMS Tx Profile 238
6.7.8 MAOTP - MAP MO-SMS Tx Profile Print 239
6.7.9 MARTI / MARTC / MARTE - MAP Ready for SM Tx Profile 240
6.7.10 MARTP - MAP Ready for SM Tx Profile Print 241
6.7.11 MASPI / MASPC / MASPE - MAP Subscriber Profiling Profile 242
6.7.12 MASPP - MAP Subscriber Profiling Profile Print 242
6.7.13 MATRI /MATRC / MATRE - MAP MT-SMS Rx Profile 243
6.7.14 MATRP - MAP MT-SMS Rx Profile Print 244
6.7.15 MATTI / MATTC / MATTE - MAP MT-SMS Tx Profile 245
6.7.16 MATTP - MAP MT-SMS Tx Profile Print 246
6.7.17 MAULI / MAULC / MAULE - MAP Update Location 247
6.7.18 IPHNI / IPHNE - IP Host Configuration 248
6.7.19 IPHNP - IP Host Configuration Print 248
6.7.20 MAUPI / MAUPC / MAUPE - MAP USSD Profile 249
6.7.21 MAUPP - MAP USSD Profile Print 250
6.8 MMI Commands 251
6.8.1 MMLOI - MMI Logoff Initiate 251
6.9 Maintenance Commands 251
6.9.1 MNINE - Maintenance Uninhibit Initiate 251
6.9.2 MNINI - Maintenance Inhibit Initiate 252
6.9.3 MNPCS - Maintenance PCM Control Set 253
6.9.4 MNRSI - Maintenance Restart Initiate 254
6.9.5 MNSSI - Maintenance Snapshot Initiate 254

6.10 Message Router Commands 255
6.10.1 MRCEE - Message Router Concerned Entity End 255
6.10.2 MRCEI - Message Router Concerned Entity Initiate 256
6.10.3 MRCEP - Message Router Concerned Entity Configuration 257
6.10.4 MRCPE - Message Router Custom Profile End 257
6.10.5 MRCPI - Message Router Custom Profile Initiate 258
6.10.6 MRCPP - Message Router Custom Profile Configuration 259
6.10.7 MRDEE - Message Router Destination End 259
6.10.8 MRDEI - Message Router Destination Initiate 260
6.10.9 MRDEP - Message Router Destination Configuration 261
6.10.10 MROGE-Message Router Origin Configuration 261
6.10.11 MROGI - Message Router Origin Configuration 262
6.10.12 MROGP - Message Router Origin Configuration 262
6.10.13 MRRKI - Message Router Routing Key Initiate 263
6.10.14 MRRKE - Message Router Routing Key End 264
6.10.15 MRRKI - Message Router Routing Key Initiate 264
6.10.16 MRRKP - Message Router Routing Key Configuration 265
6.11 Measurement Commands 265
6.11.1 MSACP - ATM Cell Stream Traffic Measurements 267
6.11.2 MSCGP - Circuit Group Measurements 268
6.11.3 MSCRP - SS7 Route Measurements 269
6.11.4 MSDBP – Subscriber Database Service Measurements 269
6.11.5 MSDEP - Message Router Destination Measurements 270
6.11.6 MSDHP - DTS Host Measurements 271
6.11.7 MSFEP - Flow Environment Measurements 272
6.11.8 MSHLP - Host Link Measurements 273
6.11.9 MSHPP - Diameter Peer Measurements 274
6.11.10 MSLCP - Software License Capability Measurements 274
6.11.11 MSLTP - SCCP Loadshare Table Measurements 275
6.11.12 MSMLP - SS7 Monitor Link Measurements 276
6.11.13 MSNIP - Network Interface Measurements 277
6.11.14 MSOGP - Message Router Origin Measurements 278
6.11.15 MSPCP - PCM Measurements 279
6.11.16 MSRAP - SIGTRAN Remote Application Server Measurements 280
6.11.17 MSRKP - Message Router Routing Key Measurements 280
6.11.18 MSRLP - Remote Server Link Measurements 281
6.11.19 MSSLP - SS7 Link Measurements 282
6.11.20 MSSRP - SIGTRAN Route Measurements 284
6.11.21 MSSTP - SIGTRAN Link Measurements 284
6.11.22 MSSYP - System Measurements 285
6.11.23 MSHRP - MAP HLR Rx Measurements 286
6.11.24 MSHTP - MAP HLR Tx Measurements 288
6.11.25 MSORP - MAP MO-SMS Rx Measurements 289
6.11.26 MSOTP - MAP MO-SMS Tx Measurements 290
6.11.27 MSRTP - MAP Ready for SM Tx Profile Measurements 291
6.11.28 MSSPP - MAP Subscriber Profiling Measurements 292
6.11.29 MSTRP - MAP MT-SMS Rx Measurements 293
6.11.30 MSTTP - MAP MT-SMS Tx Measurements 295
6.11.31 MSUPP - MAP USSD Measurements 296
6.12 Reset Commands 297
6.12.1 RSBOI - Restart Board Initiate 297

6.13 Status Commands 298
6.13.1 STBOP - Board Status 299
6.13.2 STCGP - Circuit Group Status 299
6.13.3 STCRP - SS7 Route Status 300
6.13.4 STDDP - Disk Drive Status 301
6.13.5 STDBP – Subscriber Database Service Status 301
6.13.6 STDEP - Circuit Group Device Status 302
6.13.7 STDHP - Status DTS Host Print 303
6.13.8 STFEP - Flow Environment Status 304
6.13.9 STHPP - Diameter Peer Status 305
6.13.10 STHLP - Host Link Status 305
6.13.11 STIPP - IP Node Status 306
6.13.12 STLCP - Software License Capability Status 307
6.13.13 STMLP - SS7 Monitor Link Status 308
6.13.14 STNIP - Network Interface Status 309
6.13.15 STPCP - PCM Status 310
6.13.16 STRAP - SIGTRAN Remote Application Server Status 311
6.13.17 STRLP - Remote Server Link Status 312
6.13.18 STSLP - SS7 Link Status 312
6.13.19 STSRP - SIGTRAN Route Status 313
6.13.20 STSSP - SCCP Subsystem Resource Status 314
6.13.21 STSTP - SIGTRAN Signaling Link Status 315
6.13.22 STSWP - System Software Status 316
6.13.23 STSYP - System Status 316
6.13.24 STTDP - TCAP Dialogue Status 317
6.13.25 STTPP - NTP Server Status 318
6.13.26 STTRP - TCAP Resource Status 319
6.13.27 STUAP - User Account Status 319
6.14 Command Parameters 320

7 Configuration Guidelines 367
7.1 Overview 367
7.2 IP Port Bonding 367
7.3 Sharing Licensed Throughput Between Protocols and Networks 368
7.4 Configuring Multiple Network Contexts 368
7.4.1 Multiple Network Support 368
7.4.2 Support for Multiple Local Point Codes 369
7.4.3 Protocol Handling for Multiple Network Contexts 370
7.4.4 RMM 371
7.4.5 MTP 371
7.4.6 M3UA 371
7.4.7 ISUP 372
7.4.8 SCCP 372
7.4.9 DTS 373
7.4.10 TCAP 373
7.4.11 MAP 374
7.4.12 IS41 374
7.4.13 INAP 375
7.5 Dual Resilient Signaling Server Operation 375
7.5.1 Configuring a Dual Signaling Server Pair 376
7.5.2 Hardware Requirements 376
7.5.3 System Configuration 377
7.5.4 Changes to the config.txt Parameter File 377
7.5.5 Configuring a Dual Resilient System 385

7.6 Configuring an ANSI System 385
7.7 Specifying Default Routes 386
7.8 Dynamic Host Activation 386
7.9 Dynamic Configuration 387
7.9.1 Config.txt-Based Dynamic Configuration 387
7.10 SIGTRAN M2PA Signaling 388
7.10.1 Overview 388
7.10.2 M2PA License 388
7.10.3 SS7 over M2PA 388
7.10.4 Configuration Examples 388
7.11 SIGTRAN M3UA Signaling 389
7.11.1 Overview 389
7.11.2 Configuration Examples 389
7.12 SIGTRAN M3UA - Dual Operation 391
7.13 ATM Configuration 391
7.13.1 Overview 391
7.13.2 Configuration Example 391
7.14 Simultaneous MAP/INAP/IS41 Operations 392
7.15 GTT Configuration 393
7.15.1 Global Title Address Information 393
7.15.2 Examples 394
7.16 HSL Signaling 396
7.16.1 MTP_LINK - IFTYPE 397
7.16.2 MTP_LINK - OPTIONS 397
7.16.3 MTP_LINK - TS 397
7.17 Monitoring 398

Revision History

Date	Issue No.	Description
October 2014	11	Improved alarm reporting for MMI and SNMP. Support for database services. Minor corrections and enhancements. Support for BorderNet™ Diameter Services Helix.
April 2014	10	Minor corrections and enhancements. Addition of statement that this manual is also used for BorderNet™ Diameter Services Helix.
December 2013	9	Minor corrections and enhancements.
November 2013	8	Addition of support for IPV6 and Message Router Functionality. Addition of new format config.txt commands that support entry of parameters in any order, allow optional parameters to be omitted and enhance readability by using format ParameterName=ParameterValue. Additional OA&M enhancements.
August 2013	7	Minor corrections and enhancements including support for DTS routes and dynamic GTT configuration.
June 2013	6	Minor corrections and enhancements. Support for cumulative licensing.
August 2012	5	Minor corrections and enhancements. MMI Command descriptions now make reference to the location the command can be accessed using the Web browser.
April 2012	4	Minor corrections and enhancements. Support for additional commands introduced in SWS release 1.1.0.
February 2012	3	Minor corrections and enhancements. Additional guidelines for Dual Resilient Signaling Server operation.
September 2011	2	General Availability.
July 2011	1	Initial version for Beta release.

1 Overview

1.1 Introduction

The *Dialogic® DSI Signaling Servers SS7G41 Operators Manual* provides instruction to install and operate the Dialogic® SS7G41 Signaling Server (also referred to herein as "SS7G41 Signaling Server" or "Signaling Server" or simply "SS7G41") and the BorderNet™ Diameter Services Helix (also referred to herein as "BorderNet Diameter Services Helix" or "BorderNet DSH" or simply "DSH").

The BorderNet DSH and the SS7G41 share a common user interface and this manual is relevant for both products. The manual covers installation commissioning and operation including full details of all the user commands. The SS7G41 and BorderNet DSH each use of a subset of the management and configuration interface commands for System, IP, SIGTRAN, and SS7 protocol as detailed in this manual.

The manual offers detailed information on the initial installation, licensing, provisioning and administration while operating in SIU and SWS modes and defines the full set of provisioning and administration commands as well as diagnostic and alarms indications required by operators for maintenance purposes.

SS7G41 SIU Mode

An SS7G41 with the SIU Mode software license installed and enabled, operates as a Signaling Interface Unit (SIU) providing an interface to SS7 networks for a number of distributed application platforms via TCP/IP LAN. In this mode an application developed by the user can use the Dialogic® DSI message API to interface with the SS7 or SIGTRAN protocols (MTP3, M3UA, ISUP, BICC, SCCP, TCAP, MAP, IS41 and INAP) operating on the unit. In addition, when fitted with Dialogic® DSI SS7 Boards, the SIU can be used to build high performance monitoring applications. For a detailed description and use of the system acting as a Signaling Interface Unit, see the *Dialogic® DSI Signaling Servers SS7G41 SIU Developers Manual*.

An SS7G41 with SIU Mode software license installed and enabled may also be configured to operate as a Message Router. The Message Router capability provides the ability to flexibly route messages between the Network Domain (MTP or M3UA), User Parts and Sigtran Application Servers using M3UA. The routing is based on the MTP routing label and allows messages from a specific Origin to use individual Routing Keys to selectively match routing label parameters and determine which Destination to be sent towards. The Message Router can be configured to act as a Sigtran Signaling Gateway or basic Signaling Transfer Point (STP). The Signaling server can also behave as an SCCP Router by configuring the Message Router to send traffic through the local SCCP for Global Title Translation. For further information on Message Router configuration and operation, see the *Dialogic® DSI SS7G41 Signaling Server Introduction to Message Router Functionality*.

SS7G41 SWS Mode

An SS7G41 with the SWS Mode software license installed and enabled combines a Web Services interface and service-oriented APIs with powerful message processing, providing an interface to SS7 and SIGTRAN networks for one or more client applications. In this mode, the unit provides a high level RESTful API to MAP service functionality operating on the server allowing rapid development for mobile applications such as SMS, USSD and Location Based services. For a detailed description and use of the system acting as a Signaling Web Server, see the *Dialogic® DSI Signaling Servers SS7G41 SWS Developers Manual* and *Dialogic® DSI SS7G41 Signaling Server Introduction to SWS Profiles*.

BorderNet DSH

The BorderNet DSH combines Diameter Routing Agent (DRA), Diameter Edge Agent (DEA) and Interworking Functions (IWF) together with flexible AVP manipulation capabilities.

Key Features of the product include Diameter routing, security, load balancing and interworking. Protocol support includes any to any multi-protocol interworking and service manipulation at the AVP level. Flexible connections into SS7 and SIGTRAN networks are offered by the product based on the functionality shared with the SS7G41 SIU product.

Message and AVP manipulation can be performed on both Diameter and non-Diameter messages offering multiple logical and conditional operations. This functionality can be combined to provide a flexible service creation environment.

Extensive protocol support includes Diameter, Radius, MAP, HTTP and LDAP. Refer to the *BorderNet™ Diameter Services Helix User Manual* for further details.

1.1.1 Related Information

Refer to the following for related information:

- *Dialogic® DSI Signaling Servers SS7G41 Hardware Manual*
- *Dialogic® DSI Signaling Servers SS7G41 SIU Developers Manual*
- *Dialogic® DSI Signaling Servers SS7G41 SWS Developers Manual*
- *Dialogic® DSI Components Software Environment Programmer's Manual (U10SSS)*
- *Dialogic® DSI Signaling Servers SNMP User Manual (U05EPP)*
- *Dialogic® DSI SS7G41 Signaling Server Introduction to SWS Profiles (GA20LGD)*
- *Dialogic® DSI SS7G41 Signaling Server Introduction to Message Router Functionality (GA17LGD)*

Information about the Dialogic® DSI Signaling Server products are available from the following:

http://www.dialogic.com/support/helpweb/signaling

The following manuals should be read depending on the protocol options installed on the unit:

- *ISUP Programmer's Manual (U04SSS)*
- *SCCP Programmer's Manual (U05SSS)*
- *TCAP Programmer's Manual (U06SSS)*
- *MAP Programmer's Manual (U14SSS)*
- *IS41 Programmer's Manual (U17SSS)*
- *INAP Programmer's Manual (U16SSS)*
- *SCTP Programmer's Manual (U01STN)*
- *M3UA Programmer's Manual (U02STN)*
- *M2PA Programmer's Manual (U03STN)*

1.1.2 Applicability

This manual is applicable to the SS7G41 with SIU release 2.2.x or later; or SWS release 2.0.x or later. This manual is also applicable to BorderNet Diameter Service Helix Releases 1.2.0 or later.

1.2 Capacity

This section identifies key capacity of the Signaling Server. The capabilities of a Signaling Server is dependent on the number and type of signaling boards installed as defined by the product variant as well as which software licenses installed.

Use of Signaling Servers in dual pairs increases the capacity of the overall system while still acting as a single SS7 point code. The numbers given in this section are for a single Signaling Server.

1.2.1 SS7G41 Common Capabilities

The table below provides the SS7G41 capacities that are in common between the SIU and SWS modes of operation.

Feature or Protocol	Capacity
Dialogic® DSI SS7 Network Interface Boards	Up to 2 x SS7LDH4 board or 2 x SS7MDL4 board
PCM per board	4 per SS7LDH4 or 4 per SS7MDL4
Ethernet interface	4
SS7 links per board	16 per SS7LDH4 or 124 per SS7MDL4
HSL links per board	4 per SS7MDL4
ATM Cell Streams per board	4 per SS7MDL4
ATM QSAAL Links per board	124 per SS7MDL4
M3UA links	Up to 512 link (equivalents*)
M2PA links	Up to 512 link (equivalents*)
SS7 linksets	120
SS7 links	256
SS7 routes	4096
Remote Application servers	256
M3UA routes	4096
Network contexts	4

Note: * For SIGTRAN links A ‘link equivalent’ is the equivalent to the use of a 64kb/s link at a maximum loading of 0.6 Erlang. Individual user deployments may exhibit different characteristics from this in which case it may be necessary to provision more or less capacity accordingly.

1.2.2 SS7G41 Capacities - SIU Mode

The table below provides the SS7G41 capacities in SIU mode.

Feature or Protocol	Capacity
ISUP / BICC	Up to 65,535 CICs, 2048 circuit groups.
SCCP	Up to 512 Local sub-systems, remote sub-systems, or remote signaling points.
TCAP	Up to 1,048,576 simultaneous active dialogs
MAP	Up to 65,535 simultaneous active dialogs
IS41	Up to 65,535 simultaneous active dialogs
INAP	Up to 65,535 simultaneous active dialogs
Hosts	Up to 128 hosts

1.2.3 SS7G41 Capacities - SWS Mode

The table below provides the SS7G41 capacities in SWS mode.

Feature or Protocol	Capacity
HTTP Support	HTTP, HTTPS
Web-service API	RESTful API over HTTP
HTTP content	XML (XSD provided)
MAP Service APIs	SMS (Mobile Originated, Mobile Terminated) USSD Location

2 Licensing, Installation, and Initial Configuration

2.1 Software Licensing

Functional capabilities and signaling protocols are activated on the Signaling Server through the use of software licenses. The following section provides information on the purchase of software licenses as well as information relating to temporary operation of the Signaling Server without software licenses.

The Software licenses supported on the SS7G41 Signaling Server are identified in Section 2.1.2, “Supported Licenses” on page 20.

For details on the licenses supported by the BorderNet DSH and how to obtain them, please contact your normal sales channel.

2.1.1 Purchasing Software Licenses

1. Place an order using your normal sales channel, quoting the product ID for the software option required. At this point in the process, there is no need to know details of the specific Signaling Server on which the option is to be installed (the target Signaling Server).

   The order ships through the normal supply channels and you will receive a paper License Certificate. The certificate contains the license terms for using the Signaling Server software option and a unique License ID that is needed to activate the license.

2. When the License Certificate is received, you should first read the full terms of the software license:
   - If you do not agree with the software license terms, contact your sales channel for a refund. You must not activate the software license.
   - If you agree the software license terms, you can continue with Step 3.

3. The next stage is to identify the Dialogic® DSI Signaling Server product(s) on which the software option is to be activated. To do this, you need to obtain the UNIT ID for the Signaling Server which is done by executing the CNSYP MML command on the target Signaling Server.

4. Once you have the License ID and the UNIT ID, the license can be activated on the Signaling Server. License Activation is the process of submitting the License ID and UNIT ID so that a License File can be generated and sent for installation on the target Signaling Server.

   The License Activation process is web-based, and the License File is sent by email. To activate the license perform the following steps:

   a. Visit the following web site:
   http://membersresource.dialogic.com/ss7/license/license.asp

(or an alternative URL if listed on the License Certificate).

   b. Provide the following information:
   - Name
   - Company
   - Country
   - Email address (this will be used to send the License File)

c. Provide the following information about the Signaling Server:

— Operating System - Enter "Signaling Server".

— Host ID - Enter the UNIT ID.

— User machine identification - A string, typically the Signaling Server name, used by you to identify the unit. This may be any value relevant to you, for example, "SIU_TEST_UNIT1".

d. Provide the License ID (taken from the License Certificates) for each protocol that is to be licensed on the target Signaling Server.

e. Submit the form. You will receive confirmation that your request has been submitted. Subsequently, you will receive your License File by email.

2.1.2 Supported Licenses

SS7G41 SIU Software License SKUs

Part#	Product ID	Description
G06-092	SS7SBG40SIU8	SIU - 8 link equivalents (TDM or SIGTRAN) *
G02-092	SS7SBG40SIU16	SIU - 16 link equivalents (TDM or SIGTRAN) *
G07-092	SS7SBG40SIU32	SIU - 32 link equivalents (TDM or SIGTRAN) *
G03-092	SS7SBG40SIU64	SIU - 64 link equivalents (TDM or SIGTRAN) *
G04-092	SS7SBG40SIU128	SIU - 128 link equivalents (TDM or SIGTRAN) *
G05-092	SS7SBG40SIU256	SIU - 256 link equivalents (TDM or SIGTRAN) *
G01-093	SS7SBG40TCAP	SIU – TCAP
G02-093	SS7SBG40MAP	SIU – MAP
G03-093	SS7SBG40IS41	SIU - IS-41
G04-093	SS7SBG40INAP	SIU – INAP
G05-093	SS7BG40DSE	SIU-DSE Interface

Note: * SIU licenses include the MTP3, M2PA, M3UA, SCCP, BICC and ISUP protocol layers.

SS7G41 SWS Software License SKUs

Part#	Product ID	Description
G06-094	SS7SBG40SWSM8	SWS: Messaging/Location - 8 link equivalents (TDM or SIGTRAN)
G02-094	SS7SBG40SWSM16	SWS:Messaging/Location - 16 link (equivalents*)
G07-094	SS7SBG40SWSM32	SWS: Messaging/Location - 32 link equivalents* (TDM or SIGTRAN)
G03-094	SS7SBG40SWSM64	SWS:Messaging/Location - 64 link (equivalents*)
G04-094	SS7SBG40SWSM128	SWS:Messaging/Location - 128 link (equivalents*)
G05-094	SS7SBG40SWSM256	SWS:Messaging/Location - 256 link (equivalents*)

* For SIGTRAN links A 'link equivalent' is the equivalent to the use of a 64kb/s link at a maximum loading of 0.6 Erlang. Individual user deployments may exhibit different characteristics from this in which case it may be necessary to provision more or less capacity accordingly.

Note: SWS licenses include the MTP3, M2PA, M3UA, SCCP, TCAP, and MAP protocol layers.

2.1.3 Cumulative Licensing

It is possible to purchase multiple licenses and combine their capabilities so that the licensed capabilities of the Signaling Server can be enhanced. For example, a SS7SBG40SIU16 and a SS7SBG40SIU32 license can be purchased and combined to create a 48 link equivalent SIU license.

To combine licenses, enter multiple License IDs when using the License Activation form at:

http://membersresource.dialogic.com/ss7/license/license.asp

If one or more licenses have already been activated and additional license(s) are being added to extend the capabilities of the Signaling Server, the License IDs for ALL licenses must be entered.

Licenses may be activated in any combination, but the Signaling Server cannot licensed beyond its maximum capabilities. Only licenses of the same operating mode may be combined, SS7SBG40SIUnn licenses cannot be combined with SS7SBG40SWSnn licenses.

2.1.4 Temporary Licenses

A temporary software license can be issued for a spare or backup signaling server in the event that an existing server encounters a problem that requires the unit to be repaired or replaced. Alternatively, a new permanent license, based on the licenses from the failed unit, can be issued for a spare signaling server.

The process for obtaining a temporary license file is almost identical to that of activating a new license. On the web based activation form, the License IDs should be prefixed with the following 4 characters: BAK-. For example, if the license ID on the certificate is G40-TCAP-785-9187, the license ID specified on the web form for the corresponding temporary license would be BAK-G40-TCAP-785-9187. The Host ID entered on the form is that of the replacement system on which the license will be installed. A temporary license file will then be sent to the email address you specify during the license activation.

A temporary license will allow operation of a spare/backup unit for a period of 30 days from date of issue, after which the system software cannot be restarted. It is therefore important to seek authorization to re-activate the original license(s), to perform the new activation, and to install the new license file prior to the expiry of the 30 day period.

2.1.5 Evaluation Mode

Signaling Server protocols are available on the unit for 1 hour in an unlicensed evaluation mode. After this period, the system will automatically re-boot and return to normal operation supporting only the capabilities that are licensed on the system. To activate an evaluation mode, the unit should be restarted as follows:

```
MNRSI:RESTART=EVALUATION,SYSTYPE=SIU;
```

Or

```
MNRSI:RESTART=EVALUATION,SYSTYPE=SWS;
```

The “Evaluation mode” alarm will be active whenever the system is operating in this mode.

2.2 Installation

Caution: The Signaling Server should only be installed by suitably qualified service personnel. Important safety and technical details required for installation are given in the appropriate system hardware manual.

In order to complete the installation of the Signaling Server unit, proceed as follows:

1. Optionally connect a VT100 terminal to the unit (see Section 2.2.1) or connect to the system using telnet and default IP address (see section Section 2.2.2).
2. Set the IP addresses of the unit (see Section 2.2.3).
3. Check whether a software download and upgrade is required (see Section 2.2.4).
4. Install any additional protocol software option licenses that you may have purchased. (see Section 2.2.5).
5. Check that the system is the correct operating mode (SIU or SWS for the SS7G41 or DSH for the BorderNet DSH). This is achieved using the MMI command CNSYP. The resulting output shows the operating mode, which is either “SIU”, “SWS”, “DSH”, or “TEST”.
6. If the operating mode is not correct and needs to be changed, this can be achieved by restarting the software with the following MNRSI command, for example:

   ```
   MNRSI:SYSTYPE=SIU;
   ```
7. Apply the configuration to the unit (see Section 4.2.5, “Configuration Procedure” on page 43). See also Chapter 7, “Configuration Guidelines” for some example configurations.

In SIU mode, the Signaling Server is typically used in a complete system with one or more host platforms but may also be used standalone for Message Router applications. In SWS mode, the Signaling Server can work with one or more Web Service Clients. The BorderNet DSH does not require and application host or Web Service Client.

2.2.1 Connecting a VT100 Terminal

A VT100 compatible terminal can be connected, using a cable to the DB-9 serial port on the rear of the unit. After pressing the carriage return (Enter) key, the Signaling Gateway interface prompt is displayed. Default serial port settings are 9600 baud, 8 data bits, 1 stop bits and no parity bits.

The output on the VT100 screen is similar to the following:

```
SS7G41(SIU) logged on at 2011-01-20 14:52:29
<
```

The user should then configure the initial IP address shown in Section 2.2.3, “Initial IP Configuration” on page 24.

2.2.2 Connecting via Telnet

The Signaling Server should be connected to the Ethernet network using an RJ-45 (10/100/1000 BASE-T) cable.

The Signaling Server is configured with a default IP address of 192.168.0.1. If this address is not suitable for access then the user should connect to the server using a vt100 session (see section 2.2.1).

The Ethernet connection should be verified by attempting to ping the Signaling Server from a computer connected to the same Ethernet network, using the following command:

```
ping 192.168.0.1
```

If the Signaling Server is connected correctly, it responds to the ping and the host machine displays a message confirming communication with the Signaling Server (the exact format and response of this message is operating system dependent).

Once ping shows that the Ethernet connection is valid, it should be possible to access the management interface. This is achieved by establishing a telnet session to port 8100, 8101, 8102, or 8103.

Note: It is not possible to telnet to the standard telnet port 23.

For example, on a typical host console, the following command starts a telnet session to an Signaling Server with an IP address of 192.168.0.1:

```
telnet 192.168.0.1 8100
```

A password is mandatory for access to the MML interface. Initially the system is configured with a single user account ‘siguser’ and for initial login the password ‘siguser’ is required. Once logged in new accounts may be created and passwords set. See section ‘Access Control and Security’ for more information on the management of user accounts.

A user opening a telnet session to the MML interface is therefore prompted to enter the ‘siguser’ password, for example:

```
SS7G41(SIU) logged on at 2011-07-06 12:32:01
user: siguser
password: *******
<
```

Telnet print commands output a number of lines of text before prompting a user to “Press return to continue or Ctrl-X to cancel”. The number of lines of output can be specified on the CNSYS command using the LINES parameter. When LINES is set to 0 this paging mechanism is disabled.

Telnet sessions timeout and logoff after a period of inactivity, by default 30 minutes. This timeout period can be changes by using the TLO parameter on the CNSYS MMI command.

2.2.3 Initial IP Configuration

Once connected to the Signaling Server via VT100 or telnet a user can then proceed to set the IP configuration of the Signaling Servers.

The IP address and subnet mask are set by entering the IPNIC system configuration command. For example, to set the IP address to 192.168.0.1 with a subnet mask of 255.255.255.0, enter the following command:

```
IPNIC:NETIF=ETH0,IP4ADDR=192.168.0.1/24;
```

The management interface also allows an IP gateway address to be specified using the GATEWAY parameter in the IPGWx command. For example, to configure a default gateway with address to 192.168.0.255, the following command is used:

```
IPGWI:IPGW=1,GATEWAY=192.168.0.255,IPNW=DEFAULT;
```

The current settings may be displayed by entering the appropriate commands:

```
IPNIP;
IPNIP:NETIF=ETH0;
IPGWP;
```

The configuration is displayed in the following format:

```
<ipnip;
Network Interface Configuration
NETIF   LABEL
eth0
eth1
eth2
eth3
EXECUTED

<ipnip:netif=eth0;
Network Interface Configuration
NETIF      eth0
IP4ADDR    192.168.0.1/24
IP6ADDR
BOND       NONE
LABEL
EXECUTED

<ipgwp;
IP Gateway Configuration
IPGW    GATEWAY                                 IPNW
0       192.168.0.255                           DEFAULT
EXECUTED
```

The new IP address parameters are initialized *with immediate effect*. If the IP address used to login to the unit for the telnet session is changed, you are automatically logged out of the session. You can however login again without delay using the new IP address.

> ***Note:*** Network infrastructure may introduce a delay while MAC addresses and newly configured IP addresses are reconciled.

The Ethernet connection should be verified by attempting to ping the Signaling Server from a computer connected to the same Ethernet network, using the following command:

```
ping 192.168.0.1
```

If the Signaling Server has been configured correctly, it responds to the ping and the host machine displays a message confirming communication with the Signaling Server (the exact format and response of this message is operating system dependent).

If ping fails, check that the IP address was entered correctly and that there is no fault with the cabling to the Signaling Server.

Note: The Signaling Server uses a static routing method for associating IP networks with Ethernet interfaces. In a network with multiple theoretical routing paths between an IP address on the Signaling Server and IP address on the network, the Signaling Server may transmit packets **to** an IP address through a different interface to that which receives packets **from** that same IP address. It is therefore quite possible for the Signaling Server to be unable to route packets back to an IP address if a connection associated with the destination IP address is lost.

2.2.4 Software Download

Current information and Dialogic® DSI Signaling Server software downloads can be found at the following URL:

http://www.dialogic.com/support/helpweb/signaling

Your product left the factory with fully functional software installed. You are however recommended to check the above URL for any recent revisions, and install them before putting the product into service.

Since it is possible to source units from multiple supply channels, we recommend that each is checked to verify that all units in a delivery are at the same software revision. Proceed as follows:

1. Check the current software version running in the system (see the CNSWP MML command in Chapter 5, “Configuration Commands”, for more information).
2. Check the latest distribution file available for the SS7G41 from the Dialogic® Signaling and SS7 Products download web site:
   http://www.dialogic.com/support/helpweb/signaling
3. If a download is required, then store the distribution file in an empty directory of your hard drive.
4. Follow steps below to update the system software.

2.2.5 Updating System Software

Unit software may be updated by FTP or SFTP transfer or from USB.

Current information and file downloads for the units can be found at the following URLs:

SS7G41 Signaling Server

http://www.dialogic.com/support/helpweb/signaling

BorderNet DSH

http://www.dialogic.com/products/diameter-signaling-controller/bordernet-diameter-services-helix.aspx

Although updating the software is not a requirement and units are expected to function well with the software supplied with them, it is recommended that you use the latest version of the software available.

Updating the Software by FTP or SFTP Transfer

Note: Secure FTP users will (by default) log into the parent directory of siguser and will then need to change to the ftpuser directory before commencing the following operation. Most Secure FTP clients provide an option to configure the default initial directory. If available, users may choose to use this instead of manually changing to the ftpuser subdirectory.

The procedure to update the system software by FTP or SFTP Transfer is as follows:

1. Establish an FTP or SFTP session.
2. Since this software is a binary file, set the FTP or SFTP transfer mode to “BINARY”.
3. Transfer the mode specific software. For example, for an SIU software binary by typing:
   ```
   put ss7g40-siu.tgz
   ```
   Note: The Signaling Server uses a case-sensitive file-system.

   Note: Different operating modes have different binary file names. For example, the filename for BorderNet DSH is helix.tgz.
4. The FTP or SFTP session should then be terminated by entering the “quit” or “bye”.
5. Establish a MML session and restart the unit by typing “MNRSI;”.

   Note: If you need to switch to a different mode after applying licenses, the command to use is: MNRSI:SYSTYPE={SIU/SWS/DSH}; specifying one of the appropriate SYSTYPE parameter values;
6. The machine then boots.
7. Once the upgrade is complete, the machine is accessible via MMI and the upgrade version can be checked using the CNSWP command.

Updating Software from a USB

The procedure for updating the system software from USB is as follows:

1. Copy the software binary distribution file to the USB memory device.
2. Insert the USB memory device into the USB port on the front of the unit.
3. Restart the unit using the front panel reset button, or by entering the MNRSI; MMI command.
4. The system will reboot until you are presented with the MMI command prompt.
5. Check the software version using the CNSWP command.
6. Remove the USB device from the USB port.

2.2.6 Installing Software Licenses

This section describes how additional licenses are installed on a Signaling Server. Each Signaling Server is licensed to run specific components of the protocol stack. The STLCP command provides a printout that shows which components are licensed on a particular unit. Each unit is uniquely identified by a unit identity value, which is displayed as the UNITID parameter in the CNSYP command output.

For the SS7G41 SIU or SWS, the License File purchased is a simple text file. The contents of the file are similar to the following:

```
SERVER localhost 0015B2A25066
VENDOR dialogic
USE_SERVER
FEATURE SIU_G40 dialogic 1.000 permanent 4 HOSTID=00aabbccddee \
    SIGN=" AAAA AAAA AAAA A6B6 17AC 42B4 1783 6300 B6A2 BF86 6AA8 \
    507A 61A7 883E AAAA"
```

The BorderNet DSH license file is not the same as the SS7G41 and the two license file formats are different.

Installing the License by FTP or SFTP Transfer

The procedure to install a license by FTP or SFTP transfer is as follows:

Note: Secure FTP users will (by default) log into the parent directory of siguser and will then need to change to the ftpuser directory before commencing the following operation. Most Secure FTP clients provide an option to configure the default initial directory. If available, users may choose to use this instead of manually changing to the ftpuser subdirectory.

The license file should be installed on the Signaling Server product(s) as follows:

1. Rename the purchased FTP/SFTP license file to sgw.lic (SIU/SWS) or helix.hlx (BorderNet DSH only).
2. Establish an FTP/SFTP session.
3. Set the FTP/SFTP transfer mode to “ASCII”, since the license file is a text file.
4. Transfer the software license to the Signaling Server by typing the command, for example, “put sgw.lic sgw.lic”.

   Note: The Signaling Server uses a case-sensitive file system. Therefore, it is necessary to specify sgw.lic in lowercase.
5. Terminate the FTP/STP session by entering “quit” or “bye”.
6. Establish an MML session and restart the unit by typing the MNRSI command. The machine then boots and completes the upgrade. Once the upgrade is complete, the machine is accessible via the MML interface.
7. Check the licenses using STLCP command.

If the licensing upgrade fails, the unit restores the previous licensing level. Further licenses can be added at a later date.

2.3 Configuration

Once the system architecture and protocol configuration is known, it is necessary to set this configuration in the Signaling Server by editing the config.txt file. See Chapter 7, “Configuration Guidelines” for details. This can be transferred to the Signaling Server via FTP or SFTP.

Installing the Configuration by FTP or sFTP Transfer

The procedure to install a configuration by FTP or SFTP transfer is as follows:

Note: Secure FTP/STP users will (by default) log into the parent directory of siguser and will then need to change to the ftpuser directory before commencing the following operation. Most Secure FTP clients provide an option to configure the default initial directory. If available, users may choose to use this instead of manually changing to the ftpuser subdirectory.

1. Establish an FTP/STP session.
2. Set the FTP/STP transfer mode to “ASCII” since the configuration file is a text file.
3. Transfer the configuration to the Signaling Server by typing the command “put config.txt config.txt”.

   Note: The Signaling Server uses a case-sensitive file system. Therefore, it is necessary to specify config.txt in lowercase.
4. Terminate the FTP/STP session by entering “quit” or “bye”.
5. Establish an MML session and restart the unit by typing the MNRSI command. The machine then boots and modifies the configuration. Once the modification is complete, the machine is accessible via the MML interface.

   Note: This procedure may also be used to update/overwrite previous configuration files.

Once the Signaling Server has been configured, the host software should be installed and configured on each application platform.

3 Access Control and Security

3.1 Concepts

The Dialogic® SS7G41 Signaling Server incorporates a number of features relating to secure access and administration of the equipment which are introduced in the following sections.

- System Policy
- Access Control
- IP Security

3.2 System Policy

The system policy defines the level of security enforced for a various aspects of the Signaling server, covering SSH, FTP/SFTP, Browser based management access, Web Services and Passwords.

3.3 Access Control

The Signaling Server supports the addition and removal of specific user accounts.

All Management Logins require a password to be entered.

Individual accounts can be granted specific access rights for Web, Telnet and FTP access allowing, for example, a particular user to be granted only ‘read’ access while another user is granted full administrative access.

Passwords for individual user account can be time limited and after expiry users will be required to specify a new password before being granted access to system management.

3.4 Access Rights

A user who has administrative privileges will be able to add or delete user accounts as well as assign access privileges for FTP, MMI and SWS access. Access rights are grouped into three categories, Interface Rights, Management Rights and Characteristics.

- Interface Rights
  - — CLI – Telnet/Serial support mmi management access.

    Note: If CLI access is granted for a user they do not need to enter a password for serial access.
  - — ossh/ftp - The ability to log on and read diagnostics as well as upload files via ftp/sftp. Support the ability to telnet in over ssh for mmi management access.

    Note: telnet/ssh operation can only be made mandatory if the Signaling Server is run in ‘secure’ mode.

— Management Web Server - The ability to access mmi/sws management using Web Management Server.

Note: Password access via the management server can only be made mandatory if the Web Server is run in 'secure' mode.

— Web Services API Web Server - The ability to use Web Services.

Note: Password access via the Web Services API server can only be made mandatory if the Web Server is run in 'secure' mode.

- Management Rights
  - — The ability to view files in the ftpuser account using the Web Management Interface.
  - — The ability to read mmi/sws configuration, status and measurements.
  - — The ability to change/add/delete mmi/sws configuration.
  - — The ability to perform mmi maintenance actions (block/unblock/reset).
  - — Account management access to add/remove users and set system time.
  - — System policy access. This access right allows the user to define the security policy for the server (e.g., allow 'weak' password, mandate password expiry, mandate password expiry length, ftp server and mmi secure access, etc).
- Characteristics
  - — Password can be set expire.

3.4.1 User Account Management

The Signaling Server supports the configuration of multiple user accounts. Using the management interface it is possible to initiate, change or remove a user account from the server, or to display the configuration data for the user account.

3.4.2 User Access Profiles

A user with system administration access is able to define a set of User Access Profiles. On creation of a User Account the system administrator can then assign a particular User Access Profile to a User to give them the level of access they require. For convenience a number of predefine profiles are created at system initialization. These may be added to or deleted as required by the Administrator.

Within each defined profile, access may be granted or denied for the following:

Category	Description
CLI	Telnet/Serial support for mmi management access.
FTP	The ability to log on and read diagnostics as well as upload files via ftp/ sftp. Support the ability to telnet in over ssh for mmi management access.
MWS	Management Web Server - The ability to access mmi/sws management using Web Management Server.
WSS	Web Services API Web Server - The ability to use the Web Services API.
MGR	The ability to read mmi/sws configuration, status and measurements. The ability to view files in the ftpuser account using the Web Management Interface.
MGW	The ability to change/add/delete mmi/sws configuration.

MGX	The ability to perform mmi maintenance actions (block/unblock/reset).
MGA	Administrative access to add/remove users and set system time.
MGP	System policy access. This access right allows the user to define the security policy for the server (e.g., allow 'weak' password, mandate password expiry, mandate password expiry length, ftp server and mmi secure access, etc).
EXP	Whether the password in the account should expire.

For each profile it is possible to control management privileges for specific categories of system administration and configuration.

Category
Configuration Read
Configuration Update
System Maintenance
System Security
System Administration
Policy Management

3.5 Security

3.5.1 HTTP Access

HTTP access can be restricted to secure HTTPS access only for both the browser based management interface and for web services access in SWS mode.

For HTTPS access, an SSL certificate is required. Supported SSL certificates for HTTPS are OpenSSL '.PEM' files, without a passphrase.

To load a certificate, the certificate file should be named either "MGMT.PEM" or "WSAPI.PEM" and uploaded to the ftp account. This certificate will be installed and used when the system is restarted. The file will be removed from ftp account once installed. Certificates may also be loaded via portable media (USB).

3.5.2 Firewall

The Signaling Server incorporates an IP Firewall that may be configured to only allow access via specific IP address or networks. Detail related to IP firewall configuration and operation is provided in the IP Firewall commands (IPFWP, IPFWI, IPFWC, IPFWE).

3.5.3 SSH

For additional security, the Signaling Server supports the use of Secure Shell (SSH) tunneling for telnet and secure FTP operation.

> ***Note:*** The unit does not provide a Secure Shell session connection. Your SSH client may need additional configuration to allow SSH tunneling without a session connection.

Once activated, a future user is required to set up an SSH tunnel prior to telnet access. For a client on a Linux- or Solaris-like operating system, log in for telnet using the ssh application. The ssh application should be invoked using a shell script of the following form:

```
#!/bin/sh

ssh -l siguser -C -f $1 -L 2323:$1:8101 sleep 5

telnet localhost 2323
```

For a client on a UNIX operating system, the command sequence to log in for FTP access using the sftp application is:

```
sftp -l siguser@<Signaling Server IP Address>
```

You are also prompted to enter the password for the siguser login account.

The secure connection to a unit can also be established from other operating systems, using the appropriate SSH software.

3.5.4 Configuring Public-Key Authentication for SSH

Configuring for Public-Key Authentication allows the operator to use SSH to connect to the Signaling Server without using a password. For security reasons this is recommended where the connection is made using a script.

This process requires an RSA or DSA key-pair generated for each Host. Refer to the documentation for the SSH package for more information.

- Using Secure FTP to connect to the Signaling Server.
- If the ".ssh" directory does not exist in the user directory, create one.
- Create a text file and add the Public Key for each Host on a new line.
- Upload the file to ".ssh/authorized_keys".
- Ensure the permissions on the ".ssh" directory and its parent directory "ftpuser" are set to "750".

Ensure the permissions on ".ssh/authorized_keys" are set to "640".

It is recommended that the first connection using the Public-Key Authentication method be made manually.

When using SSH or Secure FTP to connect to the Signaling Server, specifying the Private-Key will allow you to log in as without using the password.

3.5.5 SSH Tunneling for RSI

When operating in SIU mode, to protect RSI traffic between the SIU and SIU-Host the SIU-Host may be configured to use an SSH tunnel to transport the RSI traffic to the SIU.

The configuration of the SSH Client on each SIU-Host depends on the SSH package used. The following instructions show a suggested configuration method for both Linux and Windows operating systems. For both systems, it is recommended that the first connection is made manually, to allow the Client accept the SWS Host Key.

Using Linux and OpenSSH

The following script initiates a single SSH tunnel. The SSH Client exits, rather than attempting to re-establish the tunnel, should the IP link be interrupted or the SIU restarted, so the loop ensures that the SSH client is restarted. This configuration may also be used with Solaris and Sun SSH.

```
tunnel.sh contains:
#!/bin/sh
#tunnel.sh - configures a SSH tunnel to the SWS ($1).
while true
do
 ssh -l ftpuser -i ~/.ssh/priv_key -N -C -L 9000:$1:9000 $1
done
```

The tunnel script is started, prior to starting the GCT environment, with the command:

```
./tunnel.sh <SWS IP Address>
```

4 System Management

The Signaling Server supports the MMI Console.

A console based interface over telnet or serial port to configure and manage the system. Also provides easy access to diagnostic and statistics from the system. This manual provides a complete definition of the MMI commands and parameters as well as providing examples of their use.

- Web-Interface

The Web management interface provides an alternative management interface the MMI console. This interface architecturally sits on top of the MMI interface and is intended to provide the user with a graphical alternative to that interface. The Web management interface is intended to be essentially self-documenting.

- FTP

FTP and SFTP access is supported allowing users to upload system configuration files and software updates as well to retrieve diagnostic information from the Signaling Server.

- SNMP

A SNMP interface supporting v1, v2 and V3 SNMP allowing a user to query system status as well as supporting the ability to report SNMP traps.

- Lights Out Management

The Lights Out Management Interface enables a user to check the status of the equipment without the system software running.

4.1 Web Interface

The web management interface of the Signaling Server can be reached using a Web browser with IP of Ethernet port 0 as the URL, for example the following:

http://192.168.0.1

For compatibility and security reasons it is recommended that an up to date Web browser client should be used to access the Server.

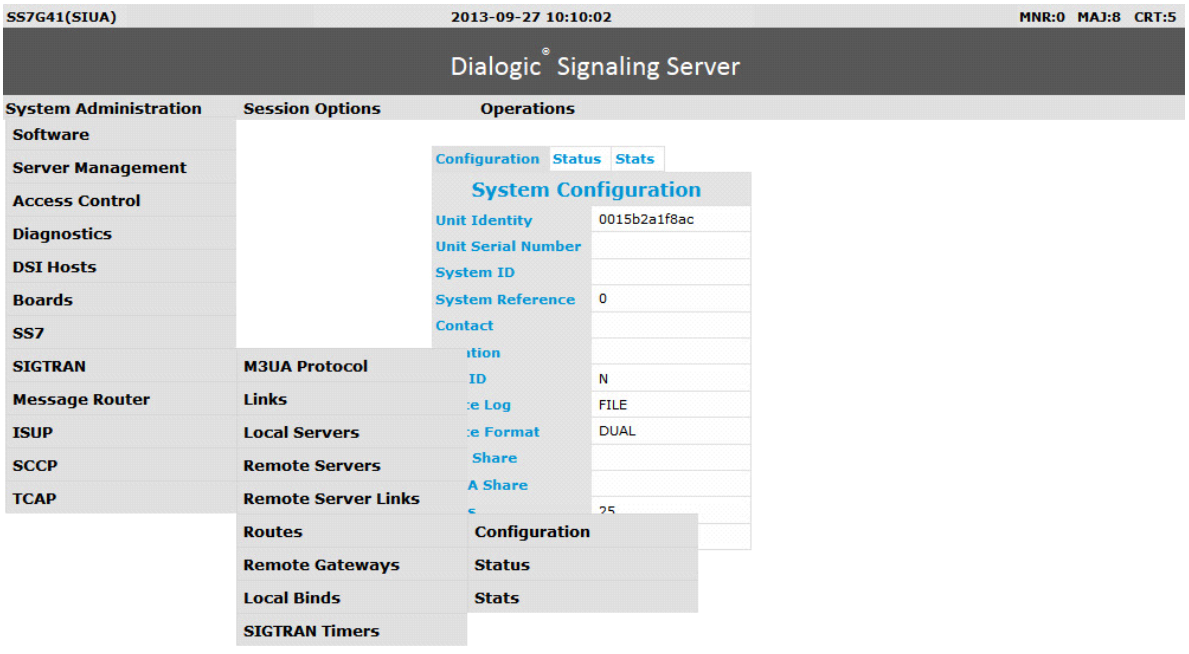
Access to the Web Interface may be restricted several ways including the following:

- Access can be restricted to the use of https
- Access to the Web Server on the system handling the web management interface may be configured so that a user must enter a user name and password before they can gain entry.
- Once access has been gained a user is then required to enter a user name and password for access to a management session.
- Functional areas of such as configuration update and control may be restricted to particular users limiting other user to read only access.

See Chapter 3, “Access Control and Security” for more detail of Management of Access to the Web interface.

Once a user has entered the URL of the Signaling Server on a Web browser they will either optionally be requested to enter their user name and password or they will presented with the default landing page of the Signaling Server. This landing page requests a that a user login for a management 'session'. Up to eight users may log into the Web interface at a time. A user will automatically be logged out after a period of time if the system detects there has been no activity in the browser session. The screenshot below shows the session landing page:

Once a user has logged into a session the follow appears:



A page on Web management interface consists of the status bar, a Navigation and Control bar and a data table. The data tables report the same configuration, status and measurements that are provided over the MMI interface.

The Status bar provides a summary of the system status and includes the system ID, the current time on the Signaling Server and a count of the number of Minor, Major and Critical Alarms.

On the Navigation and Control bar, there are a number of entries that provide the following functionality:

- System Administration – The System Administration field allows a user to navigate to a particular object such as PCMs, SIGTRAN links etc. which when selected will change the page to a table presenting configuration, status and measurements (where available).
- Session Options – The session options allow the user activate/deactivate the following particular capabilities for the lifetime of a session.
  - Help – When activated hovering the mouse above any command/parameter will result in a popup help window offering further information.
  - Compressed Format. By default parameter names are longer and more easily understandable than the MMI equivalents. Setting compressed format changes the names to the MMI version.
  - Files – When activated a new element on the Navigates and control bar is created ‘files’. Once active, if a user has permission to read the ftp user directory they can then use the files menu to navigate to a particular file such as the config.txt or a copy of this manual in the main ftp login directory or any of the syslog subdirectories in the FTP account that contains diagnostic information such as logs of MMI commands, traces, PCAP logs system logs etc.
  - No Confirm. Some actions such as add/removing blocking on a object table generate a pop-up ‘are you sure’ box. Setting the ‘No confirm’ option disables this.
  - Auto-Refresh. When set the web page will automatically refresh every 10s when viewing status and measurements.
- Operations – Operations are a set of links to some of the more frequent actions that a user may perform on the system such as log-off, restart, Diagnostic snapshot as well as shortcuts to the alarm and initial landing pages. A user may also use the 'New Session' operation to open a new browser tab or window accessing the management interface or, when DUAL operation is active, a new session can be opened on the partner Signaling Server. Finally, a user may request that the config.txt file be restored to its default values.
- Flow Management (BorderNet DSH only) – This menu offers control of the DSH Flow Design and Management functionality as well as Routing and DSH-specific OAM and diagnostic functionality. See Section 4.1.1, “DSH Flow Management Menu” on page 37 for an overview of this menu or the *BorderNet™ Diameter Services Helix Flow Management Manual* for further details.

The object tables themselves report all the data such as configuration, measurements and status that are associated with an object. Particular objects also allow actions such as add/delete, change, block and reset.

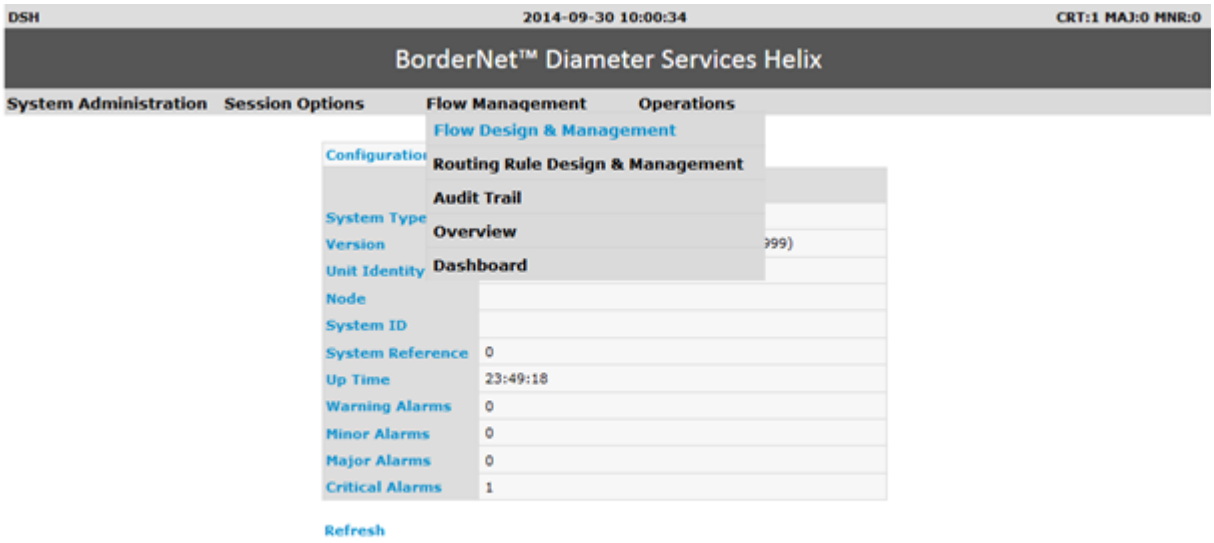
4.1.1 DSH Flow Management Menu

This menu offers access to the DSH Flow Management and Routing control functionality.

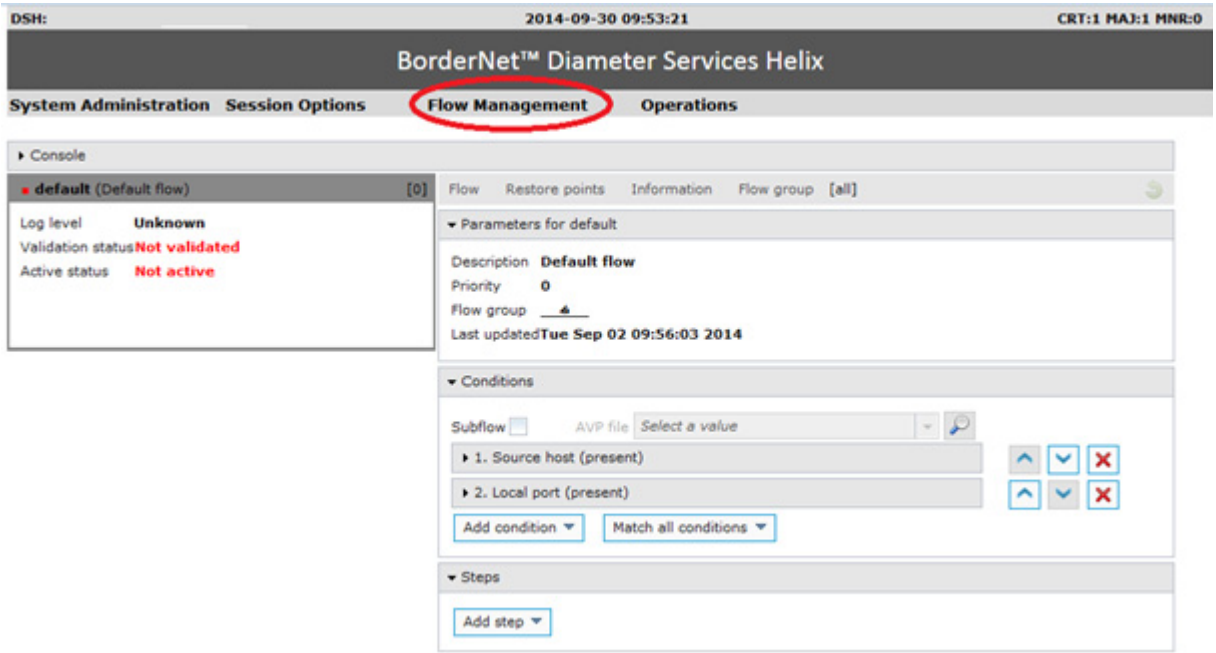
- Flow Design and Management – Flexible flow configuration and message manipulation at the AVP level for multiple protocols.
- Routing Rule Design and Management – Allows control of Diameter based routing actions
- Audit Trail – View previous user actions and activity on the unit
- Overview – Provides a summary of the flows and flow status on the unit
- Dashboard – Provides system wide and flow specific graphs of transaction rates and transaction success rates.

The Flow Management and Routing functionality of the product are covered in more detail in the *BorderNet™ Diameter Services Helix Flow Management Manual*.

Note: This menu is not visible for SIU or SWS SS7G41 operating modes or for DSH when in TEST mode.



The example shown below is a sample initial view of the *Flow Design and Management* option from the *Flow Management* menu.



4.2 Diagnostics, Alarms, and Logs

The Signaling Server supports built-in real-time logging to disk of activity on the MMI interface events and errors and the selective logging to disk of diagnostic traces.

Logging to disk of MMI activity events and errors by default allows a user to capture any management information at the point a failure occurs. Selective logging to disk of traces completes the capture of all the information that may be required to investigate particular issues.

Although activation of trace logging has a performance impact on a system, customers who do not require the full performance capabilities of the Signaling Server may choose to activate selective tracing thus ensuring the full capture of any significant information required for problem analysis.

To activate selective tracing, the user should first configure where they wish the trace messages to be logged using the CNSYx command TRACELOG parameter and then configure and activate the relevant trace mask using CNTMx commands. TRACELOG, by default, will be set to log trace messages to local FILE. The user can, however, modify the TRACELOG configuration to either transmit the messages to the management module on the management HOST or to DUAL to log locally as well as transmit to the management host.

Events and errors will be logged to files of the name “maint.log” in the syslog/maintenance sub-directory of the user account. These files will be limited to be a maximum of 5 MB with support being provided for up to 10 files. When the maint.log file reaches the 5 MB limit, or the system is restarted, it will be renamed maint.log.1 and a new maint.log file will be created. If there is an existing maint.log.1 file that will be renamed maint.log.2, other log files will consequently be renamed in a similar manner with the oldest file maint.log.9 being removed.

MMI inputs and outputs will be logged to files of the name "mmi.log" in the syslog/mmi sub-directory of the user account. In the same manner as the maintenance logs, these files will be limited to be a maximum of 5MB with support being provided for up to 10 files.

Alarm events will be logged to files of the name “alarm.log” in the syslog/alarms sub-directory of the user account. In the same manner as the maintenance logs, these files are limited to be a maximum of 5MB with support being provided for up to 10 files.

When configured, trace messages will be logged to files of the name “trace.log” in the syslog\trace sub-directory of the user account. Just as event, alarm and MMI logs, logs of these files are limited to be a maximum of 5MB with support being provided for up to 10 files. Finally, trace messages for M3UA and MTP3 may also be logged in PCAP file format producing files of the name “trace.pcap” in the same manner as above. PCAP logging is selected using the TRACEFMT parameter in the CNSYx MMI command.

Upon restart, the Signaling Server also backs up the existing system configuration and generates additional diagnostic files. These files, together with the maintenance and optionally trace log files may aid the support channel in the analysis of events and errors occurring on the Signaling Server.

These logs can be collected together into a single file using the MNSSI MMI command. This command is also available on the Operations table on the Web Interface.

Once executed a copy of these log files, together with a snapshot of the system status, will be stored in a snapshot.tgz file in the ftpuser ftp account directory. The file can then be copied of the system using FTP or SFTP for offline inspection.

4.3 Automatic MMI Logging

To allow for audit of user MMI sessions, all user dialogues are logged to a rolling log file to permit subsequent review of the command history. The text format log files include all MMI commands, responses and events.

Log files are created in the 'syslog' sub-directory of the siuftp account. The most recent file is called mmi.log and older files are called mmi.log.1, mmi.log.2 and so on up until mmi.log.9. The capacity of each file is limited to prevent disk overflow.

Each entry in the file includes the date and time of the event. For security the text value of the PASSWORD and CONFIRM parameters are replaced by the string "******".

4.4 Alarm Listing

The system maintains a record of active alarms and a log of historic alarm events. Alarm information can be accessed in several ways including:

- Display to screen
- Access using SNMP (either on request or through trap notifications)
- Export of a CSV-formatted text file

The list of currently active alarms is accessed using the ALLIP (Alarm List Print) command.

The ALLOP (Alarm Log Print) command is similar to the ALLIP command except that it reports the previous 1,000 alarm events and details the time the alarm cleared.

Alarm events are also archived to the text file ‘alarm.log’ in the syslog/alarms sub-directory of the ftp account.

Each of the following alarm log fields described below are supported:

- Header
- NODE – this user-configurable field provides a short-form identity of the unit. This identity is displayed in the browser interface, on the MMI interface at login, and included on a per alarm event basis in the SNMP ALARM MIB and in the CSV-formatted alarms.log file. The field is up to 9 alphanumeric characters and is set using the CNSYS command.
- SEQUENCE – the sequential reference number of an entry in the alarm log since the last restart.
- CODE – the unique numeric identifier of the alarm code.
- STATE – the current state of the alarm, which can be Active, Acknowledged (the alarm is still active but has been acknowledged by an operator), or Cleared. The user can acknowledge an alarm using the browser interface or by using the ALLIS command by specifying the SEQUENCE parameter.
- SEVERITY – the perceived severity of the active alarm.
- ID – the numeric identifier of entity to which the alarm relates (e.g., the LINK number).
- DIAG1, DIAG2 – the additional diagnostic information provided on the occurrence of an alarm. The meaning of these fields varies based on the alarm code.
- OCCURRED – the time the alarm occurred.
- CLEARED – the time the alarm cleared.
- TITLE – the descriptive title for the alarm code.

- TYPE – the classification of the alarm into an alarm type from the following list:
    - communicationsAlarm (2)
    - qualityOfServiceAlarm (3)
    - processingErrorAlarm (4)
    - equipmentAlarm (5)
    - environmentalAlarm (6)
- CAUSE – the probable cause for the alarm code based on the principles of ITU Recommendations M.3100, X.733, X.736 and GSM 12.10 (ETS 300 618). The values used are defined in the DSMI-TC MIB.

The order of the fields in the CSV file alarms.txt are as follows:
Header,NODE,SEQUENCE,CODE,STATE,SEVERITY,ID,DIAG1,DIAG2,OCCURRED,CLEARED,TITLE,
TYPE,CAUSE

The STSYP and STSWP commands also report a summary of the count of active alarms in each of the following categories: “Critical,” “Major,” “Minor” and “Warning.”

The ALCDP command lists the supported alarm codes and their attributes that are shown in the following table.

.

Alarm IDs, Severity, Description and Clearance Actions

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
1	PCM Loss	PORTID	MAJ	Loss of signal at PCM input port. No signal detected on PCM input. Check physical connectivity and remote equipment.
2	Sync Loss	PORTID	MAJ	Loss of frame synchronization on PCM port. Check configuration settings, connectivity and remote equipment.
4	AIS	PORTID	MAJ	Alarm Indication Signal received on PCM interface (all ones on all timeslots). Check configuration, connectivity and remote equipment.
5	Remote Alarm	PORTID	MAJ	PCM port is receiving a Remote Alarm Indication. Remote end has detected an issue. Check configuration, connectivity and remote equipment.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
6	BER5	PORTID	MAJ	The input PCM signal contains a bit error rate (BER) in excess of 1 in 100,000, indicating background errors on the PCM interface. Check physical connectivity, check clocking, ensure there are no frame slips and monitor LIU measurements.
7	BER3	PORTID	MAJ	The input PCM signal contains a BER in excess of 1 in 1,000, indicating unacceptable errors on PCM interface. Check physical connectivity, configuration and remote equipment.
8	PSU failure	PSUID	CRT	Power supply has failed. Check the external power connection and check to ensure that power is switched on. If this fails to restore the fault, replace the power supply unit.
9	SS7 link fail	LINK	MAJ	Communications failure has occurred; SS7 signaling link has failed. Check configuration, connectivity and remote equipment.
10	SS7 linkset lost	LINKSET	MAJ	Communications failure has occurred; all signaling links in an SS7 signaling link set have failed. Possibly caused by incorrect configuration (point codes or signaling timeslots), connectivity fault, or inactive signaling terminal at the remote end. Check configuration, connectivity and remote equipment.
12	SS7 link cong	LINK	MNR	Traffic throughput exceeds per-link capacity. Reduce traffic load and investigate capacity of remote end or add additional links.
13	Fan fail	FAN	CRT	The system has detected a failure of one or more or its cooling fans leading to inadequate airflow. Replace the faulty fan(s).

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
14	Fan warning	FAN	MAJ	The system has detected either the failure of one of the cooling fans or that a fan is likely to fail. The cooling will remain adequate during this condition, but the fan should be replaced at the next convenient opportunity. Check that airflow ducts are free from blockage. If the fault persists, replace cooling fans.
16	Temperature	0	CRT	The internal temperature is above a preset threshold, indicating that either an internal fault or failure of the cooling arrangements. Inspection should take place immediately. Check for obstructions to cooling vents; check that the ambient temperature is within the specified range; check operation of the cooling fans; and conduct a general inspection to identify the cause.
17	Host link fail	HOSTID	CRT	Communications failure has occurred; SIU Host (Ethernet) link has failed. Check configuration, connectivity and remote equipment.
18	Partner link fail	0	CRT	Communications failure has occurred; the Inter Signaling Server link over Ethernet to the partner unit has failed. Check configuration, connectivity and remote equipment.
19	Parse errors	0	CRT	One or more syntax errors were found in the protocol configuration file. Refer to page 2 of the alarm log for further information on errors. Check the configuration file, correct errors and restart the unit.
20	Config fail	0	CRT	Errors occurred during the configuration cycle. Check configuration file, correct errors and restart unit.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
22	System Overload	0	MAJ	System overload has occurred. Current load on system exceeds the capacity the unit can support. Reduce traffic load or investigate possible fault conditions that may be causing reduced system capacity.
24	Evaluation mode	0	CRT	System is operating in evaluation mode and will restart after a period of 1 hour. To clear this alarm, obtain and install the full license.
25	CPU Temperature	CPUID	MAJ	The CPU temperature is outside a preset threshold, indicating either an internal fault or failure of the cooling arrangements. Inspection should take place immediately. If this alarm occurs, perform a hard restart of the unit. If this alarm persists, shut down the unit, and remove and reapply power. If alarm persists, contact Dialogic support.
28	Board fail	BPOS	CRT	A signaling board has failed. (Note that during the startup sequence that all boards are marked as failed). Attempt to restore operation by resetting the board. If this fails, perform a hard restart of unit. If this fails, replace the board.
30	CPU warning	0	MAJ	The system has detected that one or more of the CPUs is likely to fail. If this alarm occurs, perform a hard restart of the unit. If the alarm persists, shut down the unit, and remove and reapply power. If the alarm persists, contact Dialogic support.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
31	Voltage warning	0	MAJ	The system has detected that the voltage on one or more power rails is out of range. This is usually due to either a faulty power supply module or a faulty board causing excessive current consumption. If this alarm occurs, perform a hard restart of the unit. If the alarm persists, shut down the unit, and remove and reapply power. If the alarm persists, contact Dialogic support.
32	Memory warning	0	MAJ	Detected memory capacity is below the expected threshold. Perform a hard restart of unit. If the fault persists, contact Dialogic support.
34	Sigtran link fail	SNLINK	MAJ	Communications failure has occurred: an M3UA SIGTRAN link has failed. Check configuration, connectivity and remote equipment.
38	Traffic congested	PROTOCOLID: 20=M3UA-NC0 21=M3UA-NC1 22=M3UA-NC2 23=M3UA-NC3 30=M2PA-NC0 31=M2PA-NC1 32=M2PA-NC2 33=M2PA-NC3	MNR	Traffic throughput through the licensed module is at or near the licensed capacity. Reduce traffic throughput or obtain a higher capacity license.
39	Traffic enforce	PROTOCOLID: 20=M3UA-NC0 21=M3UA-NC1 22=M3UA-NC2 23=M3UA-NC3 30=M2PA-NC0 31=M2PA-NC1 32=M2PA-NC2 33=M2PA-NC3	MAJ	Traffic throughput through the licensed module exceeds licensed capacity. Reduce traffic throughput or obtain a higher capacity license.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
41	Restart required	0	CRT	A system restart is required before the system changes can take place. Invoke a manual restart to clear the fault.
42	System restart	0	CRT	The system is (re)starting. This condition will clear when the system is fully in service. This is a normal alarm condition during a restart that should clear after a few minutes. If the alarm persists, investigate other active alarms that should indicate the reason for a restart failure.
45	NTP sync fail	0	CRT	Failure to sync with a remote NTP server. Check configuration, connectivity, accessibility and operation of remote NTP server(s).
52	Drive unavail	DRIVE	MAJ	Hard disk drive failure. A disk drive in the RAID array is unavailable for use The drive should be replaced using a genuine spare part from Dialogic.
67	CMOS Bat Low	0	WRN	The CMOS back-up battery has discharged. Replace CMOS battery.
69	Insufficient hosts	0	CRT	Communications failure has occurred: the number of available SIU hosts is below the minimum threshold. All signaling links will have been taken out of service until a host becomes available. Check configuration, connectivity and remote equipment.
70	SDP congestion	0	CRT	Resource exhaustion has occurred within the SDP. High throughput to a remote subscriber database caused exhaustion of an internal resource. Reduce traffic level or report to Dialogic support.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
71	File sys warning	Diagnostic code.	WRN	The underlying file system has detected an issue that could not be corrected during normal startup of the system. This error can usually be cleared by a restart of the unit that causes the file system to be checked. In a suitable maintenance window, perform a hard restart of the unit. If alarm persists, contact Dialogic support.
72	DB unavail	Identity of the database, set to: (DBSVDID * 100) + DatabaseID	MAJ	Communications failure has occurred: a subscriber database is unavailable. Check configuration, connectivity and operation of remote database.
73	CRT test alarm	0	CRT	A user-activated critical alarm test has occurred. This is a test alarm that can be manually activated and cleared using the management interface.
74	MAJ test alarm	0	MAJ	A user-activated major alarm test has occurred. This is a test alarm that can be manually activated and cleared using the management interface.
75	MNR test alarm	0	MNR	A user-activated major alarm test has occurred. This is a test alarm that can be manually activated and cleared using the management interface.
76	Flow Env unavail	0	MAJ	The Flow Environment is not currently available. This condition may indicate that an internal restart of the flow environment is taking place following detection of a fatal error. If the condition persists, then it may be cleared after restart of the unit.
77	Diameter peer fail	HDPR	MAJ	Communications failure to a Diameter peer has occurred. Check configuration, connectivity and remote equipment.

Alarm IDs, Severity, Description and Clearance Actions (Continued)

CODE	TITLE	ID	SEVERITY	DESCRIPTION ALARM CLEARANCE ACTION
78	SCTP path fail	SNLINK	MNR	Communications failure has occurred on an individual path: one or more paths in a SIGTRAN association have failed. Check configuration, connectivity and remote equipment.

4.5 SIGTRAN Throughput Licensing

The SIGTRAN license installed on the unit determines the number of SIGTRAN links that can be configured on the system. For license descriptions, see Section 2.1.2, “Supported Licenses” on page 20.

Throughput is restricted through a congestion mechanism which allows a system to briefly exceed the licensed throughput - provided that the average throughput does not exceed the licensed limit. If a system exceeds the limit for a sustained period of time then the licensed limit will be enforced and traffic throttling will reduce throughput until sufficient credit is gained to return to normal operation.

Two alarms provide indications of throughput congestion and throughput enforcement. Traffic congest indicates that enforcement will be reached unless traffic is reduced, Traffic Enforce indicates that the system is actively throttling the traffic to the licensed rate. In addition, the API command API_MSG_SIU_STATUS, will provide the following indications of congestion and enforcement to the management module.

Value	Event	ID
0x2b	Traffic congestion	0
0x2c	Traffic enforcement	0
0x2d	Clearing traffic congestion and enforcement if active.	0

The MMI command, STLCP - Software License Capability Status, will report the status of the licensable capabilities of the system such as protocols or different modes of operation. The command will report whether a license is present, whether it is inactive or active, whether it is dependent on another license or requires a restart before it can become active. The STLCP command also reports the permitted throughput and remaining throughput credit. The MMI command, MSLCP - Software License Capability Measurements provides measurements showing peak and total throughput within a particular time period.

4.6 SNMP

The Signaling Server SNMP offerings provides comprehensive support for status and traps using Distributed Structure Management Information (DSMI) SNMP.

SNMP operation is disabled by default.

Activating SNMP

SNMP support can be activated for the following:

- SNMP operation (if licensed) by setting the CNSNS MMI command's SNMP parameter to DSMI.

The server should be restarted using the MNRSI command to activate the SNMP agent.

4.6.1 DSMI SNMP

DSMI SNMP functionality allows the configuration of V1 (RFC 1157), V2c (RFC 1901), or V3 (RFC2571) SNMP traps notifying external SNMP managers of alarm conditions and configuration state changes for the objects supported on the MIB.

For all objects represented within the DSMI MIB — including platform hardware components as well as configuration aspects — the MIBs will maintain current object state and alarm conditions affecting the object.

SNMP traps can be configured to report individual alarms encountered by the alarm MIB or on a per-DSMI object basis such that the remote SNMP manager is notified whenever a DSMI object (e.g., SS7 link) is created, destroyed or the object state changes. By default, per object state change traps will be generated towards a configured SNMP manager. The DSMIEVENT field on the CNSNx MMI command can be used to configure the generation of per object traps, alarm traps or both alarm and per object traps. If per object traps are configured, the CNOBx MMI command can be used to configure whether simple DSMI object state change traps are generated or both configuration as well as state change traps are sent.

For details of the DSMI SNMP MIB, supported alarms, SNMP traps and configuration refer to the *Dialogic® DSI Signaling Servers SNMP User Manual*.

4.7 Lights Out Management

Lights Out Management allows you to monitor and manage the Signaling Server remotely using a dedicated management channel, regardless of whether the server is powered on. A remote management interface is included with the Dialogic® DSI Signaling Server model.

4.7.1 Using the Remote Management Interface

The remote management interface uses the eth3 interface on the Signaling Server and has the following default IP network configuration:

- IP address: 192.168.0.2
- Subnet mask: 255.255.255.0
- Gateway: none

The eth3 interface is shared between the operating system and the management module. The interface has two MAC addresses and two IP addresses, but only one cable is connected to it. See the *Dialogic® DSI Signaling Servers SS7G41 Hardware Manual* for details on the Ethernet interfaces.

To access the remote management interface, follow these steps:

1. Assign IP address 192.168.0.100 to the computer that will access the remote management interface.
2. Connect this computer to eth3 on the Signaling Server either directly using a crossover cable, or connect through a standalone Ethernet hub or switch.
3. Enter the following URL from a Microsoft Internet Explorer or Mozilla Firefox browser on the computer:
   http://192.168.0.2

You are redirected to secure HTTP (HTTPS) connection. A message related to the web site's security is displayed. You can click to continue to the web site, or you can install a security certificate on the system.

1. Log into the remote management interface using the following information:

- User: siguser
- Password: siguser

The System Information page is displayed.

2. Click **Remote Control** in the top menu bar.
3. To launch the redirection console viewer, click **Console Redirection**.

Note: You will need to install the Java Runtime Environment to use this option.

4. To see the server power status and perform power control functions, click **Power Control**.
5. The following power control functions are available:

- Reset Server
- Power Off Server - Immediate
- Power Off Server - Orderly Shutdown
- Power On Server
- Power Cycle Server

4.7.2 Changing the IP Address of the Remote Management Interface

The remote management interface (Lights Out Management) IP address can be configured from within that interface itself. Once logged into the default 192.168.0.2 you can change the IP address on the “configuration>network” menu.

Note: Management and configuration of the Lights Out Interface is purely within the interface itself and wholly separate from Signaling Server Management Tools.

4.8 Hard Disk Management

4.8.1 Hard Disk Drive RAID Management

The SS7G41 systems are equipped with 2 mirrored hard disk drives configured in RAID 1 array (Redundant Array of Independent Disks). These disks will remain synchronized, ensuring that an up-to-date copy of all data on the disk drives (such as the operating system software, Dialogic® DSI signaling software, system licenses and configuration files) will be maintained on both disks. In the event of failure of a single drive, the Signaling Server will continue to support the capabilities of the Signaling Server. When the failed disk drive is replaced with a unformatted disk drive, following the procedure below, the Signaling Server will mirror the operating software and data onto the new drive.

In the event of hard disk failure, the system will alarm, identifying the disk as unavailable. The disk drive must be deactivated using the MNINI - Maintenance Inhibit Initiate command before removing and replacing the disk with a blank (unformatted) disk.

Refer to hard disk drive removal instructions in the *Dialogic® DSI Signaling Servers SS7G41 Hardware Manual*. Once the disk has been replaced it should be activated using the MNINE - Maintenance Uninhibit Initiate command at which time the system will attempt to perform a synchronization function, copying all software to the newly installed disk drive. The “disk unavailable” alarm will persist until both disk drives are synchronized. The disk unavailable alarm will persist even if a failed disk drive is removed and not replaced.

Spare hard disk drives for the SS7G41 system are available as on orderable part. Refer to the *Dialogic® DSI SS7G41 Signaling Servers Product Data Sheet* (navigate from the following for part number information):

http://www.dialogic.com/products/signalingip_ss7components/signaling_servers_and_gateways.htm

Important: Although the RAID management software has been designed to be robust, it is important to follow the removal and replacement procedures described above, in order for RAID array hard disk drive integrity.

Warning: USB storage devices should not be connected to the Signaling Server during hard disk drive removal and replacement. Verify that all attached USB storage devices are removed before performing HDD removal, replacement and re-activation.

Disk drive replacement should be performed during a scheduled maintenance period preferably with the system shutdown, or for hot swap, during a period of light traffic.
Re-synchronization of disk drives subsequent to replacement can take between 5-10 minutes, depending on the conditions and the load under which the Signaling Server is operating. The Signaling Server should not be restarted during this period and MMI activity should be limited to checking the status of the re-synchronization. The status of the disk drives can be identified using the STDDP - Disk Drive Status command.

If the disk is replaced while the system is shutdown, when the system is restarted the status of the disk will remain DOWN until synchronization is started by deactivating and reactivating the disk using MNINI and MNINE.

A status of INACTIVE indicates the disk has been deactivated by the user, a status of RESTARTING indicates that it is attempting to synchronize but the operation is not yet complete. A status of UP indicates that a disk is fully operational.

Following the RESTARTING state, if the status changes to DOWN either the replacement disk is faulty or RAID mirroring has failed due to the action of the hot swap. If this occurs, the Server should be restarted without the disk in place and the disk re-inserted once the system is operational. Synchronization is re-activated using MNINI and MNINE.

If the server is restarted through power loss or user action while synchronization is in progress, the synchronizing disk will be in an indeterminate state and on restart may cause the server to fail to boot. In such an event the disk should be removed from the server and any formatting on the disk manually removed. The disk should be re-inserted in the server and the system booted. To restart synchronization use MNINI and MNINE. Alternatively, the system may be booted without the disk in place and the disk re-inserted once the system is operational. Synchronization is re-activated using MNINI and MNINE.

Warning: Attempts to reactivate disks that have failed due to hardware reasons potentially can lead to a restart of the server. The server operates a watchdog to protect the operation of the server. If the server becomes unstable due to a failed hardware or software component, the watchdog will force a system restart to attempt to resolve the problem.

4.9 System Backup and Restoration

You can back up the system configuration, software licenses, and operating software to an archive which can be restored to the system at a later date.

At startup the system will take a copy of the following system files storing them in the syslog subdirectory of the siguser account:

File	Description
SS7g40-siu.tgz	A binary file contain SWS mode operating software, if present
Ss7g40-sws.tgz	A binary file contain SIU mode operating software, if present.
sgw.lic	A text file containing the current software licenses active on the system, if present.
modcap	A binary file containing a software license allowing Signaling Server operating software to function on this particular system.
config.CF3	A binary configuration file containing dynamically configurable data that is common to all modes of operation. Parameters set by the CNSYS command would for example be stored in this file.
config.txt	The text configuration file for an SWS or SIU, if present.

The files can be recovered from the syslog directory using FTP as detailed below:

```
ftp 192.168.0.1

user siguser
password ********
cd syslog/dist
ascii
get config.txt
get sgw.lic
bin
get sgw.lic
get modcap
get config.CF3
get SDC.CF4
cd dist
get SS7G40-SIU.tgz
get SS7G40-sgw.tgz

bye
```

The Signaling Server may be restored to the configuration and licensing stored on the portable media by inserting the portable media (USB) into the Signaling Server and re-booting. On re-boot, the system will install the files stored on USB onto the system. Configuration files present on the portable media will overwrite any in the FTPUSER directory.

Note: Once the system has been restored, you must ensure that the USB is removed from the Signaling Server, otherwise on subsequent re-boot the system will again install the files stored on portable media.

Note: You also have the ability to re-install any of the previously backed up system files (identified above) or to install a new text configuration file using FTP rather than from portable media. In this case, they should ftp the files onto the unit using the procedures defined in this manual.

5 Configuration Commands

5.1 Overview

Initial SIU protocol and physical interface configuration is determined by a text file containing the parameters that are specific to a particular installation. It is necessary for you to modify this file to configure the unit for the desired operation. After this initial configuration, the unit must be restarted before the configuration is applied. Modifications to the configuration require that the text file be updated. If the modifications are to configuration elements capable of dynamic configuration (see Section 5.1.2, “Dynamic Configuration” on page 57), an update can take place without impact to other configuration elements in the system. If the configuration command cannot be dynamically configured, the Signaling Server requires a restart before the configuration updates can take effect.

To simplify entry of IP addresses and avoid the need to type the same IP address multiple times, the user can define tokens to represent IP addresses. This is achieved using the IP_TOKEN - IP Token command. An IP host name used in the multi node configuration can be configured using the IP_HOST - IP Host Configuration command, and the multi node configuration itself can be configured using the MULTI_NODE - Multi-Node Configuration command.

The SIU_HOSTS and SIU_DUAL commands should be used to setup the environment in which the SIU will operate.

Signaling boards are configured using SS7_BOARD - SS7 Board Configuration commands with the associated PCMs configured using the LIU_CONFIG - Line Interface Configuration command.

M2PA SIGTRAN Links are configured using the STN_LINK - SIGTRAN Link Configuration command.

The MTP parameters are assigned using the MTP_CONFIG - Global MTP Configuration, MTP_LINKSET - MTP Link Set, MTP_LINK - MTP Signaling Link and MTP_ROUTE - MTP Route commands. MTP link timers can be changed from their default values using the MTP2_TIMER, MTP3_TIMER and QSAAL_TIMER commands.

The M3UA parameters are assigned using the STN_CONFIG - SIGTRAN Configuration, STN_LAS - SIGTRAN Local Application Server Configuration, STN_LINK - SIGTRAN Link Configuration, STN_RAS - SIGTRAN Remote Application Server Configuration, STN_RASLIST - SIGTRAN Remote Application Server List Configuration, STN_ROUTE - SIGTRAN Route Configuration, STN_RSGLIST - SIGTRAN Route Signaling Gateway List Configuration and STN_LBIND - SIGTRAN Local Bind Configuration commands. SIGTRAN link timers can be changed from their default values using the SCTP_TIMER, M2PA_TIMER and M3UA_TIMER commands.

When using Message Router Functionality or operating as a Signaling Gateway the message router commands (MRF_CE, MRF_OG, MRF_DE, MRF_RK and MRF_CP) are used to configure the routing model.

The configuration parameters for the telephony user part are entered using the ISUP_CONFIG - ISUP Configuration or CONFIG command, as appropriate. Circuit groups are configured using the xxx_CFG_CCTGRP commands. This allows a number of circuits to be configured with common attributes. Circuit groups are assigned unique logical identifiers, or group IDs (GID). A single gid must not be used by more than one telephony user part. The Circuit Identification Code (CIC) of the first circuit in the group is defined for each circuit group. Further circuits may be included in the group providing that the CIC of the last circuit is no more than 31 greater than the first CIC.

The SCCP protocol is configured using the SCCP_CONFIG - SCCP Configuration and SCCP_LSS - SCCP Local Sub-System Resources, SCCP_RSP - SCCP Remote Signaling Point, SCCP_RSS - SCCP Remote Sub-System Resources commands. Subsystems are assigned using SCCP_SSR. Concerned subsystems are configured using SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration.

The SCCP protocol is configured using the SCCP_CONFIG - SCCP Configuration and SCCP_LSS - SCCP Local Sub-System Resources, SCCP_RSP - SCCP Remote Signaling Point, SCCP_RSS - SCCP Remote Sub-System Resources, commands. Subsystems are assigned using SCCP_SSR. Concerned subsystems are configured using SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration.

Load share tables used by SCCP Global Title Translation are configured using the SCCP_LOAD_SHARE_TABLE - SCCP Load Share Table and SCCP_LOAD_SHARE_DPC - SCCP Load Share Table commands.

SCCP Global Title Translations are configured using the SCCP_GTT_PATTERN - Global Title Translation Pattern, SCCP_GTT_ADDRESS - Global Title Translation Address and SCCP_GTT - Global Title Translations commands.

TCAP on the Signaling Server is activated using the TCAP_CONFIG - TCAP Configuration and TCAP_NC_CONFIG - TCAP Network Context Configuration commands and may be configured with Dialog groups using the TCAP_CFG_DGRP - TCAP Dialog Group Configuration command.

Configuration for INAP and MAP users of TCAP on the Signaling Server may be entered using the INAP_CONFIG - INAP Configuration, INAP_NC_CONFIG - INAP Network Context Configuration, INAP_FE - INAP Functional Entities, INAP_AC - INAP Application Context, MAP_CONFIG - MAP Configuration and MAP_NC_CONFIG - MAP Configuration commands.

DTS users requiring more than 16 hosts should configure the number of host using the DTS_CONFIG command. DTS Routes can be configured using the DTS ROUTE command.

The configuration commands and their parameters are defined in the following sections.

5.1.1 Syntax Conventions

In the command description sections of this chapter, the text under the subheading “Syntax” shows a line in the configuration file.

The following conventions apply:

- Each line starts with a keyword and is followed by a number of <parameters>.
- Items in square brackets [ ] are optional.
- The first “*” in a line indicates that the remainder of the line is a comment with no syntactical significance to the operation of the Signaling Server.

Each <parameter> may be:

- A numeric value, specified in decimal format (for example, 1234) or in hexadecimal format by prefixing the value with “0x” (for example, 0x4d2).
- Specified as bit field values, where each bit set to 1 specifies a particular configuration option. The least significant bit is designated bit 0.
- A token, where the possible values are defined in the relevant section.

5.1.2 Dynamic Configuration

Dynamic configuration is a feature supported by the Signaling Server providing a user with the ability to add or remove configuration elements on the unit without affecting the status of other elements and without the need for a system restart.

The update to the configuration is achieved by allowing a user to:

1. Modify the configuration file and transfer it into the unit via FTP.
2. Apply the appropriate MML command to update the configuration of the unit.

This allows users to modify configuration by adding or removing resources at runtime without the need to apply a system restart to the unit. In the case that a unit restart is required, the last transferred configuration is the one that is adopted.

See Section 7.9.1, “Config.txt-Based Dynamic Configuration” on page 387 for more information.

5.1.3 Programming Circuit Group Configuration

This feature provides an alternative method for dynamic configuration by allowing a host application program to add, delete, or modify ISUP circuit groups by transmitting configuration messages directly to the ISUP protocol module running on the Signaling Server. Programmatic circuit group configuration does not affect the state of existing circuits and does not require a system restart.

5.2 Command Sequence

The configuration commands must be entered in the order specified below. The command at the top of the table should be at the start of the configuration file, with the remaining commands following in the order that they appear in the table.

Table 1. Command Summary

Command	Summary
IP_TOKEN	Configure IP Hostname tokens
SIU_DUAL	Configure dual resilient operation
SIU_HOSTS	Configure SIU host settings
SS7_BOARD	Configure signaling boards
LIU_CONFIG	Configure T1/E1 PCM network interface trunks
ATM_CELL_STREAM	Configure ATM Cell Streams
STN_CONFIG	Define network context and point code type to be used by M3UA
STN_LAS	Configure local application server
STN_LINK	Configure SIGTRAN links
STN_RAS	Define a remote application server
STN_RASLIST	Attach a list of M3UA links to a remote application server
STN_ROUTE	Define SIGTRAN routes
STN_RSGLIST	Attach a list of signaling gateways to a SIGTRAN route

Table 1. Command Summary (Continued)

Command	Summary
STN_LBIND	Associate the local application server with a remote application server or remote signaling gateway - identifying the route to reach the destination.
SCTP_TIMER	Configure SCTP Timers
M2PA_TIMER	Configure M2PA Timers
M3UA_TIMER	Configure M3UA
MTP_CONFIG	Set global parameters for MTP
MTP_NC_CONFIG	Set global MTP parameters for an SS7 Network Context
MTP_LINKSET	Define link sets
MTP_LINK	Define signaling links
MTP2_TIMER	Configure MTP2 (link) timers
MTP3_TIMER	Configure MTP3 timers
QSAAL TIMER	Configure QSAAL timers
MTP_ROUTE	Configure MTP3 routing
MTP_USER_PART	Specify a user supplied user part
MTP2_TIMER	Configure MTP2 (link) timers
MTP3_TIMER	Configure MTP3 timers
QSAAL_TIMER	Configure QSAAL timers
MONITOR_LINK	Define LSL/HSL Monitor links
MRF_CE	Configure Message Router Concerned Entities
MRF_CP	Configure Message Router Custom Profiles
MRF_DE	Configure Message Router Destinations
MRF_RK	Configure Message Router Routing Keys
MRF_OG	Configure Message Router Origins
ISUP_CONFIG	Set global ISUP operating parameters
ISUP_TIMER	Configure ISUP timers
ISUP_CFG_CCTGRP	Configure ISUP circuit groups
SCCP_CONFIG	Set SCCP operating parameters
SCCP_NC_CONFIG	Set SCCP operating parameters for Network Context
SCCP_GTT	Add a translation to the SCCP global title translation table.
SCCP_GTT_ADDRESS	Define the global title to be used as the primary or backup destination of a translation.

Table 1. Command Summary (Continued)

Command	Summary
SCCP_GTT_PATTERN	Define the received global title pattern to be matched for a global title translation.
SCCP_LSS	Configure SCCP Local sub-system resources
SCCP_RSP	Configure SCCP Remote Signaling Points
SCCP_RSS	Configure SCCP Remote sub-system resource
SCCP_CONC_SSR	Configure SCCP concerned sub-system resource
MAP_CONFIG	Set MAP operating parameters
MAP_NC_CONFIG	Set MAP Network Context operating parameters
DTS_CONFIG	Set DTS operating parameters
DTS_ROUTE	Configure DTS Routes
TCAP_CONFIG	Set TCAP operating parameters
TCAP_NC_CONFIG	Set TCAP Network Context operating parameters
TCAP_CFG_DGRP	Define a range of dialogs for a TCAP host
INAP_CONFIG	Set INAP operating parameters
INAP_NC_CONFIG	Set INAP Network Context operating parameters
INAP_AC	Define INAP Application Context
INAP_FE	Define INAP Functional Entity

TCAP, MAP and INAP commands, as well as SCCP commands that relate to these protocol require a specific protocol license before they can be used.

5.3 Detection of Errors in the Configuration File

Errors detected at run time in the protocol configuration file (config.txt) are reported as “Parse Errors” in the alarm listing. Further detail on the cause of the error is available on Page 2 of the ALLIP command. This includes the line number and optional command type and parameter that are in error as shown in the following example:

```
ALLIP:PAGE=2;

Active Alarm List (Page 2 of 2)

ID    CONFIGURATION_ERROR

86    Parse error: STN_LINK unknown parameter (syntax error)

144   Parse error: MTP_LINK bad value (BLINK)
151   Parse error: MTP_ROUTE data component exists (C7RT)
```

5.4 SIU Environment Commands

The SIU environment commands include:

- IP_TOKEN – IP Token Configuration
- SIU_HOSTS – SIU Host Settings Configuration
- SIU_DUAL – Dual SIU Configuration

5.4.1 IP_TOKEN - IP Token Configuration

Synopsis

Command to create a token (IPTOKEN) to represent an IP address. The token can then be used throughout the configuration file avoiding the need to enter the full IP address in multiple places. The command can associate an IPTOKEN with and IPV4 or IPV6 address.

Applicability

SIU, SWS, DSH

Syntax

```
IP_TOKEN:IPTOKEN=,IPADDR=;
```

Examples

```
IP_TOKEN:IPTOKEN=London_ip6,IPADDR=fd77:19a9:8cf0:148:215:b2ff:fea2:4e2c;
```

Parameters

This command includes the following parameters:

- IPTOKEN

A token used within config.txt to represent an IPv4 or IPv6 address.

- IPADDR

An IPV4 or IPV6 address associated with an IP host.

Once operational additional IP tokens can be added to the config.txt file and then read into the system using the IPHNI command. IP Host names are removed from the config.txt file and then removed from the system using the IPHNE MMI command.

5.4.2 IP_HOST - IP Host Configuration

Synopsis

Command to configure an IP host.

Applicability

Operating Mode: DSH

Syntax

IP_HOST:IPHOST_NAME=,IPTOKEN=;

Example

IP_HOST:IPHOST_NAME=dsh-0015b2a48c04,IPTOKEN=Austin;

Parameters

This command includes the following parameters:

- IPHOST_NAME

A name that is used in system configuration to represent an IPv4/IPv6 address.

- IPTOKEN

A token used within config.txt to represent an IPv4 or IPv6 address.

5.4.3 MULTI_NODE - Multi-Node Configuration

Synopsis

This command configures a Node within a Multi-Node Cluster.

A Multi-Node configuration is viewed using the CNMNP command. After startup, additional nodes can be dynamically added and removed using the CNMNI and CNMNE commands.

Applicability

Operating Mode: DSH

Syntax

MULTI_NODE:MNID=,MNMODE=,IPHOST_NAME=;

Examples

MULTI_NODE:MNID=1,MNMODE=MASTER,IPHOST_NAME=dsh-0015b2a48c04;

Parameters

This command includes the following parameters:

- MNID

The Node id for nodes within a Multi-Node cluster.

- MNMODE

The mode of operation for a Node within a Multi-Node cluster. The parameter takes the following values.

STANDALONE - System operating as a Standalone Node.

MASTER - System operating as Master of a Multi-Node Cluster.

SEC_MASTER - System operating as a Secondary Master of a Multi-Node Cluster.

GROUP_MEMBER - System operating as a Group Member of a Multi-Node Cluster.

- IPHOST_NAME

A name that is used in a system configuration to represent an IPv4/IPv6 address.

5.4.4 SIU_HOSTS - SIU Host Settings Configuration

Synopsis

Command to configure settings for SIU hosts. It is used to specify the number of hosts that the Signaling Server will configure and activate as well as the host backup mode, the minimum number of hosts and the default management host.

When the command is not present in config.txt the parameters may also be configured via MMI. When configured using config.txt MMI configuration is disabled.

Configuration that has been configured using the command in config.txt will persist after it has been removed from the file and the system restarted. In this circumstance MMI can be used to change configuration.

Applicability

SIU, SWS

Syntax

```
SIU_HOSTS:NUM_HOSTS=0;

SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
```

Examples

```
SIU_HOSTS:NUM_HOSTS=0;

SIU_HOSTS:NUM_HOSTS=10,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
```

Parameters

The SIU_HOSTS command includes the following parameters:

- **NUM_HOSTS**

The number of hosts attached to the Signaling Server, in the range 0 to 128.

The specified number of hosts must be greater than or equal to the minimum number of host configured on the associated MMI command.

When NUM_HOSTS is set to 0 the Signaling Server disables all host access. NUM_HOSTS should be set to 0 when the Signaling Server is acting as a Message Router and does not require Application Hosts.

When the NUM_HOSTS is set to ALL, the Signaling Server configures the maximum number of hosts available in the system. The system will then activate the minimum number of hosts required for operation as specified by the MMI command. The rest are deactivated, allowing you to dynamically activate or deactivate them using the MNINI and MNINE MML commands. The default value for the minimum number of hosts is 1.

- **BACKUP_HOST**

The backup host algorithm, with of value of None, 0, 1 or 2 as follows:

- When this parameter is set to None or 0, the Signaling Server does not employ the backup host mechanism.
- When set to a value of 1, primary and backup hosts are paired 0-1, 2-3, 4-5 etc. If the link to host 0 fails, messages are sent instead to host 1 and vice versa. When the link recovers, normal routing resumes.

- When set to a value of 2, primary and backup hosts are paired 0-32, 1-33, 2-34 etc. If the link to host 0 fails, messages are sent instead to host 32 and vice versa. When the link recovers, normal routing resumes.

The ability to configure backup hosts allows management and/or signaling messages to be redirected to a backup host application in the event of primary host failure. When using ISUP, for example, this mechanism allows continued use of circuits if the primary host for a circuit group were to fail. Once the primary host link has been recovered, messages are again sent to it from the Signaling Server.

Backup hosts can be employed when configured for ISUP. Backup hosts may also be used for SCCP operation however, they may not be used in configurations that utilize DTS/DTC. You should ensure that both primary and backup hosts are configured and active.

- **OPTIONS**

A 32-bit value, each bit of which enables or disables additional configuration options:

  — Bit 0 - When set received MTP-Transfer-Indications will be evenly distributed across all available hosts. The distribution will be in a 'Round-Robin' manner such that the subsequent message gets routed to the next available host

  — All other bits are reserved and should be set to zero.

- **MIN_HOSTS**

The minimum number of hosts required before Network Side SIGTRAN or TDM links enter service.

- **DMHOST**

The host_id of the default management host.

SIU host configuration is viewed using the CNHSP MMI command and status and measurement for SIU host links read using the STHLP and MSHLP commands.

5.4.5 SIU_DUAL - DUAL SIU Configuration

Synopsis

Command to configure the operating mode (MODEA or MODEB) and remote IP address when operating as a dual redundant pair of Signaling Servers.

This command should be omitted if the Signaling Server is not in a dual resilient configuration.

When the command is not present in config.txt the parameters may also be configured via MMI. When configured using config.txt MMI configuration is disabled.

Configuration that has been configured using the command in config.txt will persist after it has been removed from the file and the system restarted. In this circumstance MMI can be used to change configuration.

Applicability

SIU, SWS, DSH

Syntax

```
SIU_DUAL:MODE=,REMOTE_IPADDR=;
```

Example

```
SIU_DUAL:MODE=MODEA,REMOTE_IPADDR=192.268.0.2;
```

Parameters

This command includes the following parameters:

- **MODE**

This parameter is used to select the operating mode of the unit and should be set to MODEA or MODEB. When two units are deployed in a dual resilient configuration, one unit should operate as MODEA and the other as MODEB. Changes to the parameter value require a system restart in order to take effect.

- **REMOTE_IPADDR**

The IP address of the partner Signaling Server. The IP Address may be either an IPv4 IP address or an IPTOKEN String configured to map to an IPV4 or IPV6 Address.

Signaling Server dual configuration is viewed using the CNDUP MMI command and status and measurement for the link to the partner Signaling Server read using the STRLP and MSRLP commands.

5.5 Physical Interface Commands

The physical interface commands include:

- SS7_BOARD - SS7 Board Configuration
- LIU_CONFIG - Line Interface Configuration
- STREAM_XCON - Cross Connect Configuration
- ATM_CELL_STREAM - ATM Cell Stream Configuration

5.5.1 SS7_BOARD - SS7 Board Configuration

Synopsis

The SS7_BOARD command configures a Dialogic® DSI SS7 Network Interface Board and its PCM ports.

Note: Prior to the use of this command the board must first be configured using the CNBOS MMI where the correct board type should be associated with the board and the system restarted. This configuration is required so that a physical board can be associated with a logical board position. This operation is part of the initial system configuration and therefore normally no action is required of the user. If a board is subsequently replaced however the CNBOS must be used to initially set the board type to NONE and then back to the correct board type and the system restarted so that the operating software is updated with the new hardware configuration.

Applicability

SIU, SWS, DSH

Syntax

```
SS7_BOARD:BPOS=,BRDTYPE=,OPTIONS=;
```

Examples

```
SS7_BOARD:BPOS=0,BRDTYPE=SS7LD,OPTIONS=0x0001;
```

Parameters

The SS7_BOARD command includes the following parameters:

- **BPOS**

The board position of the of the signaling board. The valid range is 0 to 1, with board 0 at the bottom of the chassis.

- **BRDTYPE**

The board type. Valid values are: SS7LD and SS7MD.

- **OPTIONS**

A 32-bit value used to configure run-time configuration options as follows:

— Bit 0 indicates the clocking mode.

When not set T1/E1 clocks are generated from the local oscillator on this board.

When set T1/E1 clocks are recovered from the highest priority T1/E1 port on this board and used as the output clock for all other ports on this board. The highest priority clock source is taken from the first configured PCM and then the next highest priority from subsequent configured ports

— Bit 16 – When set on a SS7MD board with LIUs in use for ATM operation the ATM Forum Idle cell format will be used rather than ITU.

— Bit 19 - When set the system will ensure that timestamps are always later than the previous reported timestamp. In situations where for whatever reason time is adjusted backwards the timestamps will increase at the minimal amount until the current time is again greater than the previous reported timestamp.

All other bits in the **OPTIONS** parameter are reserved and should be set to zero.

Board configuration is viewed using the CNBOP MMI command its status read using the STBOP MMI command.

5.5.2 LIU_CONFIG - Line Interface Configuration

Synopsis

This command is used to configure the PCM format used by the signaling boards.

Applicability

SIU, SWS, DSH

Syntax

```
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=E1[,LC=HDB3][,FF=G704][,CRC_MODE=NONE][,BUILDOUT=0][,OPTIONS=0]
           [,LABEL=];
```

or

```
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=T1[,LC=B8ZS][,FF=ESF][,CRC_MODE=NONE][,BUILDOUT=1][,OPTIONS=0]
           [,LABEL=];
```

Example

```
LIU_CONFIG:PORTID=0,PCM=0-1,LIUTYPE=E1;
```

Parameters

The LIU_CONFIG command includes the following parameters:

- **PORTID**

Logically identifies the PCM port on a Signaling Server. The port_id should be unique within the system and in the range 0 to 7.

- **PCM**

Identifies the physical interface to the system for LIU. It is a compound parameter, made up of board position and LIU interface number. The boards on the Signaling Server are numbered from 0 to 1, with board 0 at the bottom of the chassis. Valid values for the interface on the board are 1 to 4 for the SS7LD and SS7MD boards.

- **LIUTYPE**

Specifies the physical type of interface required according to the following table. Note that this must be selected by you to be appropriate for the actual hardware fitted otherwise, an error status is returned. This parameter must be set to one of the following values:

Value	Meaning
4	T1
5	E1 balanced
6	E1 high-impedance (for monitoring applications)
7	T1 high-impedance (for monitoring applications)
8	E1 protective monitoring point (for monitoring applications)
9	T1 protective monitoring point (for monitoring applications)

Note: Use of the Buildout parameter is not relevant when monitoring. Users are required to set it to a value of 0 when the liu type is configured for high-impedance or as a protective monitoring point.

- **LC**

The line coding technique. The following table shows the permitted values and their meaning.

Value	Description
1	HDB3 (E1 only)
2	AMI
4	B8ZS (T1 only)

- **FF**

The frame format. The following table shows the permitted values and their meaning.

Value	Description
1	E1 double frame (E1).
2	E1 CRC4 multiframe (E1).
3	F4 4-frame multiframe (T1) – SS7MD only.

Value	Description
4	D3/D4 - Yellow alarm = bit 2 in each channel (T1).
7	ESF - Yellow alarm in data link channel (T1).
8	F72/SLC96 -72-frame multiframe) (T1) – SS7MD only
9	J1 frame format (T1] – SS7MD only

- **CRC_MODE**

The Cyclic Redundancy Check (CRC*)* mode of operation. The following table shows the permitted values and their meaning.

Value	Description
1	CRC generation disabled
2	CRC4 enabled (frame_format must be set to 2)
4	CRC6 enabled (frame_format must be set to 7)

- **BUILDOUT**

Specifies the range of “build out” settings for a T1 interface. The parameter is required for SS7MD boards. The following table shows the permitted values and their meaning.

Value	Usage for SS7MD Board	Usage for SS7LD Board
0	Setting for E1 devices	Setting for E1 devices
1	T1 Default (short haul)	T1 Default (short haul)
2	T1 short haul 0 - 133 ft	T1 short haul 0 - 110 ft
3	T1 short haul 133 - 266 ft	T1 short haul 110 - 220 ft
4	T1 short haul 266 - 399 ft	T1 short haul 220 - 230 ft
5	T1 short haul 399 - 533 ft	T1 short haul 330 - 440 ft
6	T1 short haul 533 - 655 ft	T1 short haul 440 - 550 ft
7	not valid	T1 short haul 550 - 600 ft
8	T1 long haul LBO (-0dB)	T1 long haul LBO (-0dB)
9	T1 long haul LBO (-7.5dB)	not valid
10	T1 long haul LBO (-15dB)	not valid
12	T1 long haul LBO (-22.5dB)	not valid

- **OPTIONS**

A 16-bit value used to configure run-time configuration. This field is reserved for future used and should be set to 0.

- **LABEL**

Optional user configurable text string containing up to 32 characters used for identification purposes.

PCM configuration is viewed using the CNPCP MMI command and its status and measurements read using the STPCP and MSPCP MMI commands. After startup additional PCMs can be added to the config.txt file and then read into the system using the CNPCI command. PCMs are removed from the config.txt file and then removed from the system using the CNPCE MMI command.

5.5.3 STREAM_XCON - Cross Connect Configuration

Synopsis

The STREAM_XCON command controls the cross connect switch on the signaling boards, enabling the cross- connection of timeslots between the two PCM ports on each signaling board or a fixed pattern to be generated on specified timeslots. The PCM ports on a board are referenced by a fixed logical stream number.

This command is only supported for the SS7LD board.

Applicability

DSH

Syntax

```
STREAM_XCON <BPOS> <OUT_STREAM> <IN_STREAM> <XCON_MODE> <TSMASK> <OUTPUT_PATTERN>
```

Example

```
STREAM_XCON 3 2 3 3 0xfffefffe 0
```

Parameters

The STREAM_XCON command includes the following parameters:

- **BPOS**

The board position of the cross connect switch to be controlled. There must be a valid board at this position (previously defined by an SS7_BOARD command).

- **OUT_STREAM**

A reference to the 2 Mbps stream for the output of the connection or the fixed data pattern. There must be a valid PCM port at this position (previously defined by a LIU_CONFIG command). Valid values are 0 to 3.

- **IN_STREAM**

A reference to the 2 Mbps stream for the input of a simplex connection (mode 2) or one half of a duplex cross connection (mode 3). In other modes, this field should be set to zero.

There must be a valid PCM port at this position (previously defined by a LIU_CONFIG command). Valid values are 0 to 3.

- **XCON_MODE**

Indicates the requested cross connect switch function according to the following table.

Mode	Function
1	Set a fixed pattern specified by <pattern> on the output timeslot(s).
2	Connect the input timeslot to the output timeslot.
3	Duplex cross-connect the input and output timeslot.

- **TS_MASK**

A 32-bit mask specifying the timeslots to apply the cross connect or pattern to. Each bit corresponds to a timeslot in the input/output stream. Bit 0 (the least significant bit) corresponds to timeslot number 0. To apply this command to a timeslot, the corresponding bit must be set to one.

- E1 interfaces have 32 timeslots numbered 0 to 31. Timeslot 0 is used for frame alignment and timeslot 16 is generally used for signaling or is empty. Hence the normal SIU configuration is to cross connect timeslots 1 to 15 and 17 to 31 between the two ports on each signaling board by setting the TS_MASK value to 0xfffefffe.
- T1 interfaces have 24 timeslots, numbered 1 to 24. To cross connect all the timeslots on a T1 interface between the two PCM ports on a signaling board, the TS_MASK value 0x1fffffe should be used.

In duplex mode both PCM ports should have been previously configured under the same type of PCM connector E1 or T1.

- **OUTPUT_PATTERN**

One byte of fixed data to output in pattern mode (mode 1) on the output stream/timeslot. In other modes, this parameter should be set to zero.

5.5.4 ATM_CELL_STREAM - ATM Cell Stream Configuration

The ATM_CELL_STREAM command allows the configuration of ATM Cell Streams. In terms of configuration ATM Cell Streams sit above LIUs and are referred to by MTP or Monitor ATM links.

Applicability

DSH

Syntax

```
ATM_CELL_STREAM:CELLSTR=,BPOS=,L2ID=,PORTID=[,OPTIONS=0],DEFVPI=,DEFVCI=;
```

Example

```
ATM_CELL_STREAM:CELLSTR=0,BPOS=1,L2ID=0,PORTID=0,OPTIONS=0x06,DEFVPI=1,DEFVCI=6;
```

Parameters

The ATM_CELL_STREAM command includes the following parameters:

- **CELLSTR**
  The logical Cell Stream ID from the ATM module's perspective
- **BPOS**
  The board position of the signaling processor allocated for this ATM link.

- Only boards of type “SS7MD” may be associated with ATM Cell Streams.
- **L2ID**
  The Layer 2 ID of the Cell Stream within the board. In the range of 0 to one less than the maximum number of Cell Streams supported per board.
- LIU ports logical identifier(s) to be used by the cell stream. The parameter is subject to the following pre-requisites:
- LIU port specified may not be associated with any other cell stream.
- LIU port or ports must be associated with the board.

  Note: The associated timeslot bitmap of active timeslots within TDM streams for E1 is 0xfffefffe and for T1/J1 is 0x01fffffe as per G.804.

- **OPTIONS**
  A 16-bit value containing additional flags for the ATM link. The bit significance is as follows:
  — Bit 0 - Enable payload scrambling
  — Bit 1 - Use ATM coset in HEC calculation
  — Bit 2 - Autocorrect invalid cells if possible

  Note: Either Payload Scrambling or ATM Coset mode, or both, must be enabled. Payload Scrambling is a requirement G.804 operation on an E1.

- **DEFVPI**
  A default AAL5 link will be configured for the cell stream to signal incoming active connections. This is the VPI that will be used for this connection.
- **DEFVIC**
  A default AAL5 link will be configured for the cell stream to signal incoming active connections. This is the VCI that will be used for this connection. Values 0, 3 and 4 are reserved and should not be used.

ATM Cell Stream configuration is viewed using the CNACP MMI command. Cell Stream measurements read using the MSACP MMI commands. After startup additional Cell Streams can be added to the config.txt file and then read into the system using the CNACI command. Cell Streams are removed from the config.txt file and then removed from the system using the CNACE MMI command.

5.6 MTP Commands

The MTP commands include:

- MTP_CONFIG - Global MTP Configuration
- MTP_LINKSET - MTP Link Set
- MTP_LINK - MTP Signaling Link
- MTP2_TIMER - MTP2 Timer Configuration
- MTP3_TIMER - MTP3 Timer Configuration
- QSAAL_TIMER - QSAAL Timer Configuration
- MTP_ROUTE - MTP Route
- MTP_USER_PART - MTP User Part
- MONITOR_LINK - Monitor Link

5.6.1 MTP_CONFIG - Global MTP Configuration

Synopsis

The MTP_ CONFIG command defines the global configuration parameters for MTP.

Applicability

SIU, SWS, DSH

Syntax

```
MTP_CONFIG:[NC=NC0][,OPTIONS=0];
```

Example

```
MTP_CONFIG:NC=NC0,OPTIONS=0x0002;
```

Parameters

The MTP_CONFIG command includes the following parameters:

- **NC**

SS7 Network Context set to NC0, NC1, NC2 or NC3. When the parameter is omitted, a value of NC0 is used. Up to four separate Network Contexts can be configured, refer to Section 7.4, “Configuring Multiple Network Contexts” for more information.

- **OPTIONS**

A 32-bit value, each bit of which enables or disables additional configuration options:

— Bit 0 defines the operation of MTP3 when a message is received from the SS7 network with a Destination Point Code (DPC) different from the local point code configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of dpc value. This bit is normally set to zero.

— Bit 1 defines the operation of MTP3 when a message is received from the SS7 network with a sub-service field (ssf) value different from the ssf value configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of ssf value. This bit is normally set to zero.

— Bit 3 determines the behavior when a message is received from the SS7 network for a User Part that has not been configured. If set to 1, a User Part Unavailable (UPU) message is issued to the network, zero prevents the UPU from being issued. This bit is normally set to zero.

— Bit 6 controls the operation of the Signaling Route Set Test mechanism. Normally, when a remote signaling point becomes unavailable, a periodic Signaling Route Set Test message is issued in order to ensure that subsequent availability of the signaling point is detected. Setting this bit to 1 disables the sending of this message. This bit is normally set to zero.

— Bit 8 selects between ITU-T (CCITT) and ANSI operation. If set to 1, the MTP operates in accordance with ANSI T1.111, if set to 0, the MTP operates in accordance with the ITU-T (CCITT) Q.700 series recommendations.

— Bit 9 selects between 14/16-bit point codes and 24-bit point codes:
- When set to 0, 14-bit or 16-bit point codes are selected (see also Bit 20).
- When set to 1, 24-bit point codes are selected.

Note: Bit 9 must always be set to 1 for ANSI operation.

— Bit 10 is used to enable multiple congestion states.

Note: Bit 10 must always be set to 1 for ANSI operation.

— Bit 11 is used to enable Multiple Message Priority operation.

Note: Bit 11 must always be set to 1 for ANSI operation.

— Bit 16 is used to control the usage of the **hdr->id** field of MTP Transfer Indication messages:
- When set to 0, the **id** field contains the User Part Reference (or Service Indicator), this is primarily useful for backward compatibility.
- When set to 1, the **id** field provides an indication of the MTP Label Format used in the parameter area. This is the recommended setting for all new designs.

Note: Bit 16 must to be set to 1 for the mixed network ISUP configuration.

— Bit 17 controls how received Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the local point code are processed:
- When set to 0, messages are discarded.
- When set to 1, messages are sent to fixed module_id 0x0a on the host.

— Bit 18 controls MTP3 operation on detection of Remote Processor Outage (RPO):
- When set to 0, on detection of RPO, the signaling link is taken out of service and restoration commences. This setting is useful for backward compatibility.
- When set to 1, normal setting, RPO is handled in accordance with the ITU-T 1992 (and later) recommendations."

— Bit 19 is used when MTP3 is operating in dual mode to control which bit of the Sub-Service Field is used to flag messages that have been received by one MTP3 and are being conveyed to the dual module over the inter-MTP3 link set.

o 0 - Normal setting; sub-Service Field bit 2 is modified.

o 1 - Alternative setting; sub-Service Field bit 0 is modified.

— Bit 20 is used to select between 14-bit point codes and 16-bit point codes. It is only significant when 24-bit point codes are **not** selected (that is, when bit 9 is set to 0):
- When set to 0, 14-bit point codes are selected.
- When set to 1, 16-bit point codes are selected.

— Bit 21 is used to activate Japan-specific MTP3 operation:
- When set to 0, normal setting, Japan-specific functionality is disabled.
- When set to 1, Japan-specific functionality is enabled.

— Bit 22 the handling of received Route Set Test Messages. It should only be set if bit 17 is also set:
- Normal operation; Route Set Test messages processed by MTP3.
- When set to 1, messages are sent to fixed module_id 0x0a on the host.

Note: For correct Japan-specific operation, you should also select 16-bit point codes by setting bit 20 as well as bit 21.

All other bits are reserved and should be set to zero.

Note: For correct ANSI operation, bits 8, 9, 10, 11 and 18 must be set to 1. This gives a typical <options> field value of 0x00040f00 for ANSI configurations.

Note: When a Message Router Origin for a particular Network Context is configured in the NETWORK domain, Bits 0, Bit 17 and Bit 22 of the options parameter will automatically be set in the MTP_CONFIG command for the particular Network Context. These bits control how received Route Set Test, Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the MTP local point code are processed and are set to allow the Message Router to correctly process these messages for the domains and Network Contexts under its control.

5.6.2 MTP_LINKSET - MTP Link Set

Synopsis

The MTP_LINKSET command defines link sets.

Applicability

SIU, SWS, DSH

Syntax

```
MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=,SSF=[,NLINKS=1][,OPTIONS=0][,LABEL=];
```

Example

```
MTP_LINKSET:LINKSET=0,OPC=321,APC=320,LABEL=Edinburgh;
MTP_LINKSET NC=NC1,LINKSET=1,OPC=321NLINKS=2,OPTIONS=0x0000,APC=320,SSF=0x8;
```

Parameters

The MTP_LINKSET command includes the following parameters:

- **NC**

SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.

- **LINKSET**

The logical identity of the link set, in the range 0 to one less than the maximum number of link sets supported. This ID is used in other commands for reference.

- **APC**

The point code of the adjacent signaling point.

- **NLINKS**

The (maximum) number of links that are allocated to the link set. The valid range is 1 to 16.

- **OPTIONS**

A 16-bit value used to specify run time options:

— Bit 3 when set enables restart procedures for this link set.

— Bit 15 assigns special functionality to a link set for use in inter- Signaling Server communication. For a normal link set conforming to the SS7 specifications, this bit must be set to 0.

Note: Bit 15 must be set for the inter- Signaling Server link set between a Mode A Signaling Server and a Mode B Signaling server in a dual resilient configuration.

— All other bits are reserved and should be set to zero.

- **OPC**

The local signaling point code for this link set.

- **LABEL**

Optional user configurable text string containing up to 32 characters used for identification purposes.

- **SSF**

The value to be used in the sub-service field of level 3 messages for this link set. The valid range is 0 to 15. For ANSI operation, the two least significant bits (B and A) must be set to 1 to assign a message priority of 3 to all MTP3 generated messages. The remaining two bits are the network indicators (bits C and D).

Note: For correct Signaling Server operation, the adjacent point code must also appear in an MTP_ROUTE declaration.

MTP Link set configuration is viewed using the CNLSP MMI command. After startup additional Link Sets can be added to the config.txt file and then read into the system using the CNLSI command. Link Sets are removed from the config.txt file and then removed from the system using the CNLSE MMI command.

5.6.3 MTP_LINK - MTP Signaling Link

Synopsis

The MTP_LINK command allows the user to configure terminated links for HSL, LSL, M2PA and ATM signaling. The parameters required and their usage is different for each mode of operation.

Applicability

SIU, SWS, DSH

Syntax

```
MTP_LINK:LINK=,IFTYPE=M2PA,LINKSET=,REF=,SLC=[,BLINK=][,OPTIONS=0x0006][,LABEL=];
MTP_LINK:LINK=,IFTYPE=TDM,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x0006][,LABEL=];
HSL Links:
MTP_LINK:LINK=,IFTYPE=<HSLtype>,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x0006][,LABE
L=];
MTP_LINK:LINK=,IFTYPE=ATM,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=][,OPTIONS=0x00006],CELLSTR=,VPI=,VCI=[,LA
BEL=];
```

Example

```
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BLINK=0,STREAM=1,TS=16,LABEL=Dublin;
MTP_LINK:LINK=,IFTYPE=M2PA,LINKSET=2,REF=0,SLC=0,BLINK=10;
MTP_LINK:LINK=,IFTYPE=ATM,LINKSET=1,REF=2,SLC=2,BPOS=1,BLINK=5,OPTIONS=0x00000006,CELLSTR=5,VPI=4,
VCI=5;
```

Parameters

The MTP_LINK command includes the following parameters:

- **IFTYPE**

IFTYPE identifies the interface type for signaling links.

The interface mode should be set to one of the following values:

Interface_mode	Description
TDM	Single timeslot signaling link
M2PA	SIGTRAN M2PA Signaling Link
ATM	ATM Signaling Link
E1_FRAMED	Framed 31 timeslot E1 operation
T1_FRAMED	Framed 24 timeslot T1 operation
PCM	Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling)

The interface_mode value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.

- **LINK**

The links unique logical link identity within the Signaling Server. It must be in the range 0 to one less than the maximum number of signaling links supported.

- **LINKSET**

The logical identity of the link set to which the link belongs. The link set must already have been configured using the MTP_LINKSET command.

- **REF**

The logical identity of the signaling link within the link set. It should be in the range 0 to 15. This is usually be the same value set for the <slc> parameter below.

- **SLC**

The signaling link code for the signaling link. This must be unique within the link. The valid range is 0 to 15.

- **BPOS**

The board position of the signaling processor allocated for this signaling link. The board must already have been configured using the SS7_BOARD command.

Set to 0 if the MTP link is associated with an M2PA link.

- **BLINK**

For Non ATM, this is the index of the logical signaling processor (SP) channel (on the board) allocated for this signaling link.

— For Dialogic® DSI SS7LD Network Interface Boards or supporting 16 low speed signaling links, the blink parameter may be written as a single value in the range 0 to 15.

— For Dialogic® DSI SS7MD Network Interface supporting 124 low speed signaling links, the blink parameter may be written as a single value in the range 0 to 123.

— For Dialogic® DSI SS7MD Network Interface supporting 4 high speed signaling links, the blink parameter may be written as a single value in the range 0 to 3.

— When the SS7 link is to be conveyed over M2PA, the blink parameter identifies the SNLINK (link_id). When the SS7 link is to be conveyed over ATM this is the layer 2 link id.

- **STREAM**

A reference to the logical PCM highway from which the signaling processor is to insert the signaling. This must be in the range 0 to 3. Set to 0 if the MTP link is associated with an M2PA link.

Valid values are shown in the following table:

Stream	Port
0	1
1	2
2	3
3	4

- **TS**

The timeslot on the STREAM that should be used for signaling. For a T1 port, the range is 1 to 24. For an E1 port, the valid range is 1 to 31. The timeslot must not have been previously assigned another MTP or Monitor link. Set to zero if the MTP link is associated with an M2PA link.

For HSL links, the timeslot parameter should be set to 0xff to indicate that the link is attached to an LIU configured with the LIU_CONFIG command. HSL signaling may not use timeslots already configured for signaling or data.

- **OPTIONS**

A 32-bit value, each bit enabling or disabling additional run-time options:

— Bit 0 is used to signify “override automatic selection of proving period”. When set to 1, bit 3 is used to determine whether to use the EMERGENCY or NORMAL proving procedures. If set to 0, the appropriate proving period in accordance with the SS7 protocol is used.

— Bit 1 when set to 1 causes a signaling link test to be performed on link activation/restoration. If set to 0, a signaling link test is not performed. This bit should normally be set to 1.

— Bit 2 when set to 1 enables a periodic signaling link test. When set to 0, periodic signaling link tests are not automatically performed. This bit should normally be set to 1.

— Bit 3 when set to 1 forces NORMAL proving, otherwise EMERGENCY proving is used. If Bit 0 is set to 0, then the appropriate proving period in accordance with the SS7 protocol is used and Bit 3 has no influence.

— Bit 7 selects the LSSU length indicator. If set to 1, the unit sends two octet LSSU messages. If set to 0, the unit sends one octet LSSU messages.

— Bit 8 selects the error correction method used by this link. If set to 1, Preventative Cyclic Retransmission (PCR) is used. If set to 0, the basic error correction method is used. PCR is typically only used over transmission links where the transmission delay is large (such as satellite links).

— Bits 10 and 11 select either 64, 56, or 48 Kbps operation, and are used when a link operates over a T1 or E1 timeslot. Use of these bits is as follows:

Bit 11	Bit 10	Rate	Timeslot Usage
0	0	64 Kbps	Set both to zero for E1_FRAMED and T1_FRAMED operation. HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link.
0	1	48 Kbps	bits 7&8 not used
1	1	56 Kbps	bit 8 not used

— Bit 12 –sequence number length. Set to 1 the HSL signaling link will use a 12-bit sequence number. Set to 0, the HSL signaling link will use a 7-bit sequence number. 12 bit sequence numbers may not be used for LSL links.

— All other bits are reserved and should be set to zero.

— For ATM -only bits 0 to 2 are used.

- **CELLSTR**

This parameter indicates the ATM_CELL_STREAM to be used.

- **VPI**

The VPI associated with the ATM link on the cell stream.

- **VCI**

The VCI associated with the ATM link on the cell stream.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

Additional Prerequisites for ATM Operation

The VPI and VCI ranges are statically defined in the initial configuration. The VPI/VCI range must be unique for all the virtual ports, but constraints exist on the VPI and VCI value distribution as the total number of VPI/VCI and cell stream combinations must be less than 65535 (i.e., a 16bit range). By default, 3 bits are allocated for cell streams, thus 13 bits are available for the VPI/VCI address masks.

The default number of bits in the VPI address mask is 4, allocated to the lowest four bits, 0x00F, thus providing 16 valid VPIs from 0 to 15. The default for the VCI is to set the lowest nine bits of the VCI address mask, 0x01FF, thus providing 512 valid VCIs from 0 to 511 (note that VCI addresses 0, 3 and 4 are reserved).

If it is necessary to match VPI/VCI address combinations outside these ranges, then the address bit masks can be rearranged, provided that the maximum number of mask bits used is not exceeded. This can result in matching non-contiguous VCI or VPI address ranges. For example, VPI mask 0x09C will allow handling the following VPIs: 0, 4, 8, 12, 16, 20, 24, 28, 128, 132, 136, 140, 144, 148, 152, and 156.

In addition to the VPI/VCI address mask requirements, the following prerequisites should also be observed:

Non ATM signaling links cannot be associated with LIUs timeslots used by an ATM cell stream.

Up to 128 ATM signaling links can be associated with a SS7MD card.

MTP Signaling Link configuration is viewed using the CNSLP MMI command and its status and measurements read using the STSLP an MSSLP MMI commands. After startup additional Signaling Links can be added to the config.txt file and then read into the system using the CNSLI command. Signaling Links are removed from the config.txt file and then removed from the system using the CNSLE MMI command.

5.6.4 MTP_ROUTE - MTP Route

Synopsis

The MTP_ROUTE command configures a route for use with one of more user parts. Each remote signaling point must have a corresponding MTP_ROUTE entry in the configuration file, which must be entered after the MTP_LINKSET command. Using the <flags> and <second_ls> parameters, this command can configure a combined link set to a remote Destination Point Code (DPC).

An MTP route exists within a particular Network Context and may not use link sets operating within differing Network Contexts.

MTP routes can be designated as “default” routes and can be used to convey traffic for multiple destinations without the need to configure each DPC as an explicit MTP route. Typically, this is useful when a signaling point connects simply to a single STP or a mated pair of STPs and all traffic can be sent to the STP irrespective of the current network status.

Two types of default route are supported, one associated with a “real” DPC. In this case, the (default) route is deemed to be accessible whenever the specified DPC is accessible. The other associated with a “pseudo” DPC which is a point code that does not exist within the network (for example, zero). In this case the (default) route is deemed to be accessible as soon as the link sets within the route are available.

A maximum of one default route for each supported Service Indicator (or user part) is permitted.

Note: The MTP_ROUTE command must be used for each destination point code to be accessed *including* the adjacent point code. There may be only one MTP_ROUTE command for each destination.

Note: Attempting to mix, in the same configuration file, lines that use current command formats with lines that use older command formats may give rise to restart errors indicating “inconsistent command format”.

Applicability

SIU, SWS, DSH

Syntax

```
MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
```

Example

```
MTP_ROUTE:ROUTE=1,DPC=567,LS1=1,UPMASK=0x0008,LABEL=To_London;
```

Parameters

The MTP_ROUTE command includes the following parameters:

- **NC**

SS7 Network Context. This parameter identifies the SS7 network in which the route exists. The Network Context must match that of the link set(s) in the route. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.

- **C7RT**

A unique value in the range 0 to one less than the number of routes supported to identify the MTP route.

- **DPC**

The remote destination signaling point code for the route.

- **LS1**

The logical identity of the link set, in the range 0 to one less than the maximum number of link sets supported. This value is set for each configured link set in the MTP_LINKSET command.

- **UPMASK**

A 16-bit value with bit n (in the range 3 to 15) set to allow the route to be used for messages with Service Indicator (SI) n. For each user part supported, the bit corresponding to the Service Indicator for that user part should be set. For example, to enable SCCP routing (which uses an SI of 3) a value of 0x0008 should be used. To enable both SCCP (3) and ISUP (5) a value of 0x0028 should be used.

- **OPTIONS**

A 16-bit value that provides additional options:

— Bit 0 is set to 1 to enable the use of the <second_ls> parameter.

— Bit 1 is set to 1 to cause traffic sent towards the remote signaling point to be shared between the two link sets <linkset_id> and <second_ls>. If set to 0, all traffic sent towards the remote signaling point is normally sent using the link set specified by <linkset_id>, unless this link set fails, in which case the traffic uses the alternative link set <second_ls>. Loadsharing should not be configured if one of the link sets is used between a pair of Signaling Servers in a dual Signaling Server configuration.

— Bit 2 is set to 1 to indicate a default route. Messages for any DPC that is not explicitly configured use this route.

— Bit 3 is set to 1 to indicate that the DPC associated with this route is not a real DPC within the network. The route is considered available as soon as the link sets within the route are available.

Note: When bit 3 is set, bit 2 should also be set.

— Bit 5 is set to 1 to disable the Route Test procedure for this route. Typically, this bit should be set to zero. However, in the case of a “pseudo” DPC route, it is essential to set this bit to 1 to prevent RST messages being issued.

— All other bits must be set to zero.

- **LS2**

The logical identity of the second link set in the combined link set.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

MTP Route configuration is viewed using the CNCRP MMI command and its status and measurements read using the STCRP an MSCRP MMI commands. After startup additional routes can be added to the config.txt file and then read into the system using the CNCRI command. Routes are removed from the config.txt file and then removed from the system using the CNCRE MMI command.

5.6.5 MTP2_TIMER - MTP2 Timer Configuration

Synopsis

The MTP2_TIMER command provides the ability to configure the MTP2 protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
MTP2_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
MTP2_TIMER:TIMID=T4N,TMSEC=550;
MTP2_TIMER:NC=NC1,TIMID=T4N,TMSEC=550;
```

Parameters

The MTP2_TIMER command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the MTP2 timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

- **TIMID**

A text identifier for the timer to be configured. It should be set to one of the following: T1, T2, T3, T4N, T4E, T5, T6, or T7

- **TSEC**

The timer value specified in seconds.

- **TMSEC**

The timer value specified in milliseconds. Note that the timer granularity is 100ms.

Any timers not configured continue to be set to the values shown in the following table. ITU-T or ANSI selection is made by setting the value of the MTP_CONFIG options parameter.

MTP2 Timer	ITU-T 64k mode	ITU-T 48k mode	ANSI 64k mode	ANSI 56k mode	HSL
T1	45 s	45 s	13 s	13 s	300 s
T2	30 s	30 s	23 s	23 s	30 s
T3	1.2 s	1.2 s	11.5 s	11.5 s	1.2 s
T4N	8.2 s	2.3 s	2 s	2.3 s	30 s
T4E	500 ms	600 ms	500 ms	600 ms	500 ms
T5	100 ms	100 ms	100 ms	100 ms	100 ms
T6	5.5 s	5.5 s	5.5 s	5.5 s	5.5 s
T7	1.7 s	1.7 s	1.5 s	1.5 s	1.5 s

Note: The Signaling Server does not perform checks on MTP2 timer values.

5.6.6 MTP3_TIMER - MTP3 Timer Configuration

Synopsis

The MTP3_TIMER command provides the ability to configure the MTP3 protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
MTP3_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
MTP3_TIMER:TIMID=T2,TSEC=1,TMSEC=500;
MTP3_TIMER:NC=NC1,TIMID=T2,TMSEC=1500;
```

Parameters

The MTP3_TIMER command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the MTP3 Timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

- **TIMID**

A text identifier for the timer to be configured. It should be set to one of the following:
T1, T2, T3, T4, T5, T6, T10, T12, T13, T14, T15, T16, T17, T22, T23 T24, SLTC1 or SLTC2.

- **TSEC**

The timer value specified in seconds.

- **TMSEC**

The timer value specified in milliseconds. Note that the timer granularity is 100ms.

Any timers not configured continue to be set to the values shown in the following table. ITU-T or ANSI selection is made by setting the value of the MTP_CONFIG options parameter.

MTP3 Timer	ITU-T mode	ANSI mode
T1	1 s	1 s
T2	1.5 s	1.5 s
T3	1 s	1 s
T4	1 s	1 s
T5	1 s	1 s
T6	1s	1 s
T10	45 s	45 s
T12	1.2 s	1.2 s
T13	1.2 s	1.2 s
T14	2.5 s	2.5 s
T15	2.5 s	2.5 s
T16	1.8 s	1.8 s
T17	1 s	1 s
T22	270 s	270 s
T23	270 s	270 s
T24	500 ms	500 ms
SLTC T1	7 s	7 s
SLTC T2	30 s	30 s

The following timers are set to their default values and are not configurable:

MTP3 Timer	ITU-T mode	ANSI mode
T7	2 s	2 s
T8	1 s	1 s
T11	6 s	6 s
T18	20 s	20 s
T19	68 s	68 s
T20	60 s	60 s

MTP3 Timer	ITU-T mode	ANSI mode
T21	64 s	64 s
T101	2 s	2 s

Note: T9 is not used on the Signaling Server.

Note: The Signaling Server does not perform checks on MTP3 timer values.

Note: MTP timers not specified in this table are not configurable; they well be set to their specific ITU or ANSI default value.

5.6.7 QSAAL_TIMER - QSAAL Timer Configuration

The QSAAL_TIMER command provides the ability to configure the QSAAL protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
QSAAL_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
QSAAL_TIMER:TIMID=CC,TMSEC=1600;
QSAAL_TIMER:NC=NC1,TIMID=T3,TSEC=110;
```

Parameters

The QSAAL_TIMER command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network for which the QSAAL timer is being configured. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

- **TIMID**

A text identifier for the timer to be configured. It should be set to one of the following: CC, KEEP_ALIVE, NO_RESP, POLL, IDLE, T1, T2, T3.

- **TSEC**

The timer value specified in seconds.

- **TMSEC**

The timer value specified in milliseconds with a millisecond granularity.

Any timers not configured continue to be set to the values shown in the following table.

Timer ID	Default Value (ms)	Range (min – max)
CC	1,500	15 - 2,500
KEEP_ALIVE	300	15 - 2,500
NO_RESP	1,500	100 - 10,000
POLL	100	20 - 600
IDLE	100	20 - 600
T1	5,000	1,000 - 20,000
T2	120,000	10,000 - 300,000
T3	10	1-30

5.6.8 MTP_USER_PART - MTP User Part

Synopsis

The MTP_USER_PART command is used to inform the MTP that a user supplied user part exists on the host.

In dual redundant operation when a user application sends a MTP-TRANSFER-REQ intended for a MTP or M3UA network the message should be sent to a network specific Resilient MTP Manager (RMM) module rather than directly to MTP3 or M3UA. The RMM module in turn will ensure that the message is routed to the network via local MTP3/M3UA when available or the MTP3/M3UA on the partner Signaling Server if no local route is available. The per Network Context RMM modules are:

NC0 – 0x32

NC1 – OxC2

NC2 – 0xE2

NC3 – OxF2

Applicability

SIU

Syntax

```
MTP_USER_PART [<NC>] <SI> <USER_ID>
```

Example

```
MTP_USER_PART 0x0a 0x2d
MTP_USER_PART NC0 0x0a 0x2d
```

Parameters

The MTP_USER_PART command includes the following parameters:

- **NC**

SS7 Network Context. The Network Context within which this service indicator to user part association is to apply. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.

- **SI**

The service indicator for the user supplied user part in the range 3 to 15.

- **USER_ID**

The module ID of the user process that receives MTP transfer indications with the specified service indicator value.

5.6.9 MONITOR_LINK - Monitor Link

Synopsis

The MONITOR_LINK command allows the user to configure a signaling resource (e.g., blink) to monitor signaling operating between two external Switches. The type of interface being listened to is identified by the monitoring type. Received signaling messages are passed directly to a user application without further processing. The parameters required and their usage is different for each mode of operation.

Note: Often, applications that use MONITOR_LINK also require the line interfaces to operate in high impedance pr protective monitoring point mode. High impedance or protective monitoring point mode can be selected for a particular LIU using the <liu_type> parameter in the LIU_CONFIG command.

Applicability

SIU

Syntax

```
ATM Links:
MONITOR_LINK <MLINK> ATM <BPOS> <BLINK> <CELLSTR> <VPI> <VCI> <USER_ID> <USER_HOST> <OPTIONS>

HSL/LSL Links:
MONITOR_LINK <MLINK> ATM <BPOS> <BLINK> <CELLSTR> <VPI> <VCI> <USER_ID> <USER_HOST> <OPTIONS>
```

Example

```
MONITOR_LINK 1 TDM 0 1 0 1 1 0x1d 1 0x00000001
MONITOR_LINK 0 ATM 1 1 1 1 10 0x0d 0 0x00000001
```

Parameters

The MONITOR_LINK command includes the following parameters:

- **MLINK**

The monitor link's unique logical identity within the Signaling Server. It must be in the range 0 to one less than the maximum number of monitor links supported. The value must not already be allocated to another MONITOR_LINK or MTP_LINK.

- **IFTYPE**

The interface type identifies the type of object being monitored. The monitoring type should be set to one of the following values:

Interface_ mode	Description
TDM	Single timeslot signaling link
ATM	ATM Signaling Link
E1_FRAMED	Framed 31 timeslot E1 operation
T1_FRAMED	Framed 24 timeslot T1 operation
PCM	Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling)

The monitoring type value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.

- **BPOS**

The board position of the signaling processor allocated to process the incoming signaling. The board must already have been configured using the SS7_BOARD command.

- **BLINK**

For non ATM this is the index of the logical signaling processor (SP) channel (on the board) allocated for signaling link monitoring. For ATM this is the layer 2 link id.

— For Dialogic® DSI SS7LD Network Interface monitoring up to 16 low speed signaling links, the blink parameter may be written as a single value in the range 0 to 15.

— For Dialogic® DSI SS7MD Network Interface monitoring up to 124 low speed signaling links, the blink parameter may be written as a single value in the range 0 to 123.

— For Dialogic® DSI SS7MD Network Interface monitoring up to 4 high speed signaling links, the blink parameter may be written as a single value in the range 0 to 3.

When the SS7 link is to be conveyed over ATM this is the layer 2 link id.

- **BPOS2**

The board position of the stream from which the signaling is to be inserted. This parameter must have the same value as <bpos>.

- **STREAM**

A reference to the logical PCM highway from which the signaling processor is to insert the signaling. This must be in the range 0 to 3.

Valid values are shown in the following table:

Stream	Port
0	1
1	2
2	3
3	4

- **TS**

The timeslot on the <stream> that should be used for signaling. For a T1 port, the range is 1 to 24. For an E1 port, the valid range is 1 to 31. The timeslot must not have been previously assigned another MTP or Monitor link. Set to zero if the MTP link is associated with an M2PA link.

For HSL links, the timeslot parameter should be set to 0xff to indicate that the link is attached to an LIU configured with the LIU_CONFIG command. HSL signaling may not use timeslots already configured for signaling or data.

- **CELLSTR**

This parameter indicates the ATM_CELL_STREAM to be used.

- **VPI**

The VPI associated with the ATM link on the cell stream.

- **VCI**

The VCI associated with the ATM link on the cell stream.

- **USER_ID**

The module ID of the process that will receive the incoming signaling messages, passed as SS7_MSG_RX_IND messages. This should be in the range 0x0d, 0x1d … to 0xfd.

- **USER_HOST**

The logical identifier of the host to which receives SS7_MSG_RX_IND messages.

- **OPTIONS**

Per-link flags for monitoring operation. (32 bits)

— Bit 0 - Set to 1 to enable timestamping of messages monitored by the board for this link. The monitored messages are received in the API_MSG_RX_INDT message type to accommodate the timestamp as well as the received message.

— Bits 10 and 11 select either 64, 56, or 48 Kbps operation is being monitored, and are used when a link operates over a T1 or E1 timeslot. Use of these bits is as follows:

Bit 11	Bit 10	Rate	Timeslot Usage
0	0	64 Kbps	Set both to zero for E1_FRAMED and T1_FRAMED operation. HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link.
0	1	48 Kbps	bits 7&8 not used
1	1	56 Kbps	bit 8 not used

— Bit 12 - sequence number length. Set to 1 the HSL signaling link will use a 12-bit sequence number. Set to 0, the HSL signaling link will use a 7-bit sequence number.

— All other bits should be set to 0.

— For ATM -only bits 0 is used.

Additional Prerequisites for ATM Monitoring

The VPI and VCI ranges are statically defined in the initial configuration. The VPI/VCI range must be unique for all the virtual ports, but constraints exist on the VPI and VCI value distribution as the total number of VPI/VCI and cell stream combinations must be less than 65535 (i.e., a 16bit range). By default, 3 bits are allocated for cell streams, thus 13 bits are available for the VPI/VCI address masks.

The default number of bits in the VPI address mask is 4, allocated to the lowest four bits, 0x00F, thus providing 16 valid VPIs from 0 to 15. The default for the VCI is to set the lowest nine bits of the VCI address mask, 0x01FF, thus providing 512 valid VCIs from 0 to 511 (note that VCI addresses 0, 3 and 4 are reserved).

If it is necessary to match VPI/VCI address combinations outside these ranges, then the address bit masks can be rearranged, provided that the maximum number of mask bits used is not exceeded. This can result in matching non-contiguous VCI or VPI address ranges. For example, VPI mask 0x09C will allow handling the following VPIs: 0, 4, 8, 12, 16, 20, 24, 28, 128, 132, 136, 140, 144, 148, 152, and 156.

In addition to the VPI/VCI address mask requirements, the following prerequisites should also be observed:

- The cell stream must be on the same board as the signaling link.
- Non ATM links cannot be associated with LIUs timeslots used by an ATM cell stream.
- Up to 128 links can be associated with a SS7MD card.

MTP Monitor Link configuration is viewed using the CNMLP MMI command and its status and measurements read using the STMLP an MSMLP MMI commands. After startup additional Signaling Links can be added to the config.txt file and then read into the system using the CNMLI command. Signaling Links are removed from the config.txt file and then removed from the system using the CNMLE MMI command.

5.7 SIGTRAN Configuration Commands

The SIGTRAN commands include:

- STN_CONFIG - SIGTRAN Configuration
- STN_LAS - SIGTRAN Local Application Server Configuration
- STN_LINK - SIGTRAN Link Configuration
- STN_RAS - SIGTRAN Remote Application Server Configuration
- STN_RASLIST - SIGTRAN Remote Application Server List Configuration
- STN_ROUTE - SIGTRAN Route Configuration
- STN_RSGLIST - SIGTRAN Route Signaling Gateway List Configuration
- STN_LBIND - SIGTRAN Local Bind Configuration
- SCTP_TIMER - SIGTRAN SCTP Timers
- M2PA_TIMER - SIGTRAN M2PA Timers
- M3UA_TIMER - SIGTRAN M3UA Timers

5.7.1 STN_CONFIG - SIGTRAN Configuration

Synopsis

This command identifies the Network Context and point code size to be used by M3UA.

Applicability

SIU, SWS, DSH

Syntax

```
STN_CONFIG:[NC=NC0],SS7MODE=[,OPTIONS=0][,SHARE=100];
```

Example

```
STN_CONFIG:NC=NC0,SS7MODE=ITU14,SHARE=50;
STN_CONFIG:NC=NC1,SS7MODE=ITU14,SHARE=50;
```

Parameters

The STN_NC command has the following parameters:

- **NC**

SS7 Network Context. The Network Context uniquely identifies a SS7 network. Supported values are: NC0, NC1, NC2, or NC3.

SWS operation can only use NC0.

- **SS7MODE**

The SS7 mode of the network context. Possible values are:

ITU14	ITU 14 bit operation.
ITU16	ITU 16 bit operation.
ITU24	ITU 24 bit operation.
ANSI	ANSI 24 bit operation.

- **OPTIONS**

This is a 16 bit value used to specify run time options:

Bit 0 - Enables SLS bit rotation. When set, the SLS field is bit rotated after Signaling Gateway selection and prior to MSU transmission.

Bit 1 - Enables 8-bit SLS bit rotation. When set 8 bit SLS rotation will be used, when not set default SLS rotation based on MTP label format will be used. The setting of this bit is only applicable if Bit 0 is also set to enable SLS bit rotation.

All other bits are reserved for future use.

- **SHARE**

The Signaling Server support M3UA operation in multiple Network Contexts. The <share> parameter allows the user to specify the percentage (in the range 1 ... 100) of the SIU or SWS license capability that should be allocated to the specific Network Context identified by this command. The total value of <share> for all Network contexts should not exceed 100.

5.7.2 STN_LAS - SIGTRAN Local Application Server Configuration

Synopsis

This command initiates a local application server. An application server is a logical entity representing a SS7 end point.

Applicability

SIU, SWS, DSH

Syntax

```
STN_LAS:[NC=NC0],LAS=,OPC=,RC=[,TRMD=LS][,OPTIONS=0][,LABEL=];
```

Examples

```
STN_LAS:NC=NC2,LAS=1,OPC=1200,RC=1,TRMD=LS;
STN_LAS:LAS=2,OPC=1300,RC=3,TRMD=OR;
```

Parameters

The STN_LAS command has the following parameters:

- **NC**

SS7 Network Context. The Network Context together with the Originating Point Code (OPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.

- **LAS**

Logical reference for a Local Application Server. The valid range is 0-199.

- **OPC**

Specifies an Originating Point Code (OPC) value for the local Application Server.

- **RC**

The logical routing context of the local application server. An RC may not be associated with any other LAS. The valid range is 0: 2147483647.

- **TRMD**

The traffic mode for the local application Server. Acceptable values are LS (Loadshare), OR (Override) or BC (Broadcast). Only Loadshare should be used when the Signaling Server is acting as part of a dual redundant Signaling Server pair.

- **OPTIONS**

This is a 16 bit value used to specify run time options:

Bit	Description
0	When set, the configured routing context will be ignored and no routing context will be transmitted.
1-15	Reserved and should be set to zero.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

Prerequisites

SIGTRAN Local Application Server configuration is viewed using the CNLAP MMI command. After startup additional Local Application Servers can be added to the config.txt file and then read into the system using the CNLAI command. Local Application Servers are removed from the config.txt file and then removed from the system using the CNLAE MMI command.

5.7.3 STN_LINK - SIGTRAN Link Configuration

Synopsis

The SIGTRAN link configuration command supports both M2PA and M3UA SIGTRAN links.

Applicability

SIU, SWS, DSH

Syntax

```
STN_LINK:[NC=NC0],SNLINK=,SNTYPE=M3UA,RIP1=[,RIP2=],LIP1=[,LIP2=][,END=S][,LPORT=2905][,RPORT=2905][,O
PTIONS=0][,RSG=][,NA=][,LABEL=];

STN_LINK:SNLINK=,SNTYPE=M2PA,RIP1=[,RIP2=],LIP1=[,LIP2=][,END=S][,LPORT=3565][,RPORT=3565][,OPTIONS=0]
,M2PAID=[,LABEL=];
```

Examples

```
STN_LINK:SNLINK=1,SNTYPE=M2PA,RIP1=192.168.1.2,LIP1=192.168.1.1,END=C,LPORT=3565,RPORT=3565,M2PAID=1;
STN_LINK:SNLINK=2,SNTYPE=M3UA,RIP1=192.168.17.20,LIP1=192.168.17.21,END=S,LPORT=2906,RPORT=2906,OPTION
S=0x0006,RSG=1;
```

The STN_LINK command has the following parameters:

- **NC**

SS7 Network Context. The Network Context the specific SS7 network the SIGTRAN Link is operating with. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.

- **SNTYPE**

Identifies the SIGTRAN protocol and should be set to either M2PA or M3UA.

- **SNLINK**

Logical reference for a SIGTRAN link, acceptable values are 0-255. A snlink is unique to one link and cannot be re-used by another type.

- **M2PAID**

A M2PA identifier, in the range 0 to one less than the maximum number of M2PA links supported. Used for M2PA configuration only.

- **RIP1**

The primary IP address on which the Signaling Server will attempt to communicate with the remote unit. May be an IPV4 address or IPTOKEN that references a IPv4 or IPV6 address. An rip1 value of 0.0.0.0 cannot be specified.

- **RIP2**

The secondary IP address on which the Signaling Server will attempt to communicate with the remote unit. May be an IPV4 address or IPTOKEN that references a IPv4 or IPV6 address.

- **END**

Identifies whether the Signaling Server end of the SIGTRAN link acts as a CLIENT or a SERVER.

- **LPORT**

Local (Signaling Server) SCTP port in the range 1 to 65535.

- **RPORT**

Remote SCTP port in the range 1 to 65535.

- **OPTIONS**

This is a 16 bit value used to specify run time options

Bit	Description
0	Secure Mode. When set to 1, the SIGTRAN link will not come into service if it receives a message from an IP address not associated with the SIGTRAN link.
1	For a M3UA SIGTRAN link communicating with a Remote Signaling Gateway, when set to 1, a DAUD message will be sent when the link comes into service and periodically thereafter. When not set DAUD message will not be generated. Not applicable for M2PA.
2	For M3UA, set to 1 when the RSG parameter value will be used. Not applicable for M2PA.
3	For M3UA, set to 1 when the NA parameter value will be used. Not applicable for M2PA.
4	When set to zero the Signaling Server end of the link is acting as an Application Server Process. When set to one the Signaling Server is acting as a Signaling Gateway (in which case bit 2 of the options must be set to zero). When set to 1 the SIGTRAN link may only be used to connect to a Remote Application Server. Bit 3 of the associated STN_RAS command's options field should also be set.
5	When this bit is set the server ignores NA parameters in received messages. M3UA can therefore be configured to not send a NA and ignore any NA it receives.
6	When set, M3UA heartbeats will be enabled for this association.
7	When set, designates the path associated with the first remote IP address (RIP1) as the primary SCTP path that is available and will always be used.
8	When set, disables use of the Nagle algorithm to ensure that outgoing packets are transmitted without delay.
9	When set, disables the path of MTU discovery and selects a fixed MTU value of 1438.
10-14	Reserved and should be set to zero.
15	When set a M3UA link is nominated by M3UA as a 'host' link. If any SIGTRAN links have been configured as 'host' M3UA links and all these links are down then all MTP and any non 'host' M3UA links will be deactivated until at least one 'host' M3UA link returns to service.

- **RSG**

Remote Signaling Gateway (RSG). Identifies a remote server to act as a Remote Signaling Gateway. The RSG may not have the same id value as an existing Remote Application Server. No more than 32 SNLINKs can identify the same RSG. All SIGTRAN links between the Signaling Server and a Remote Signaling Gateway must be of the same protocol type.The valid range is 0-199. Used for M3UA configuration only and may only be set to a non zero value if bit 2 of the flags parameter is set.

- **NA**

The logical network appearance used in communicating with a remote server. The valid range is 0:16777215. Used for M3UA configuration only and may only be set to a non zero value if bit 3 of the flags parameter is set.

- **LIP1**

The first local IP address to be used in the association. lip1 cannot be set to 0 and cannot be the same as lip2. May be an IPV4 address or IPTOKEN that references a IPv4 or IPV6 address. If a local IP address is configured on one STN_LINK then each subsequent STN_LINK must have at least one local IP address configured.

- **LIP2**

The second local IP address to be used in the association. May be an IPV4 address or IPTOKEN that references a IPv4 or IPV6 address. It cannot be the same as lip1.

SIGTRAN Link configuration is viewed using the CNSTP MMI command and its status and measurements read using the STSTP an MSSTP MMI commands. After startup additional links can be added to the config.txt file and then read into the system using the CNSTI command. Links are removed from the config.txt file and then removed from the system using the CNSTE MMI command.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

5.7.4 STN_RAS - SIGTRAN Remote Application Server Configuration

Synopsis

This command initiates a Remote Application Server.

Applicability

SIU, SWS, DSH

Syntax

```
STN_RAS:[NC=NC0],RAS=,DPC=,RC=[,NASP=1][,OPTIONS=0][,LABEL=];
```

Example

```
STN_RAS:NC=NC2,RAS=16,DPC=14065,RC=1;
```

Parameters

The STN_RAS command has the following parameters:

- **NC**

SS7 Network Context. The Network Context together with a Destination Point Code (DPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.

- **RAS**

Remote Application Server, The Remote Application Server may not have the same ID value as an existing Remote Signaling Gateway. The valid range is **O-255.**

- **DPC**

Specifies an Destination Point Code (DPC) value for the Remote Application Server. Only one RAS, SNRT or C7RT can be configured with a particular DPC within a network context.

- **RC**

The logical routing context used in communicating with a remote server. An RC may not be associated with any other remote server. The valid range is 0: 2147483647.

- **NASP**

The number of ASP (SIGTRAN Links) required in load sharing mode.

- **OPTIONS**

This is a 16 bit value used to specify run time options:

Bit	Description
0	When set, the configured routing context will be ignored and a routing context will not be required from a received remote application server in an activate message.
2	When set to zero will consider a point code on Remote Application Servers to be unavailable if any of the Remote Application Servers have failed. When set to one will consider a point code available if any of the Remote Application Servers is in service.
3	When set to zero the Signaling Server is acting in an IPSP relationship with the Remote Application Server. When set to one the Signaling Server is acting as a Signaling Gateway for the Remote Application Server. If bit 3 is set then all associated SIGTRAN links should also have bit 4 of their STN_LINK options field set.
1-15	Reserved and should be set to zero.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

SIGTRAN Remote Application Server configuration is viewed using the CNRAP MMI command and its status and measurements read using the STRAP an MSRAP MMI commands. After startup additional Remote Application Servers can be added to the config.txt file and then read into the system using the CNRAI command. Remote Application Servers are removed from the config.txt file and then removed from the system using the CNRAE MMI command.

5.7.5 STN_RASLIST - SIGTRAN Remote Application Server List Configuration

Synopsis

This command attaches a list of SIGTRAN links to a Remote Application Server. The SIGTRAN links provide the SCTP associations to reach the Remote Application Server.

Applicability

SIU, SWS, DSH

Syntax

```
STN_RASLIST:RLID=,RAS=,SNLINK=;
```

Examples

```
STN_RASLIST:RLID=1,RAS=16,SNLINK=1;
STN_RASLIST:RLID=2,RAS=16,SNLINK=2;
STN_RASLIST:RLID=3,RAS=16,SNLINK=32;
```

Parameters

The STN_RASLIST command has the following parameters:

- **RLID**

Logical identifier for a RAS to SNLINK relationship. The valid range is 0-6399.

- **RAS**

Remote Application Server. The valid range is 0-255.

- **SNLINK**

Logical reference for a SIGTRAN Link. The SIGTRAN link cannot be M2PA, cannot be configured for communication to a RSG, and cannot be already attached to this server. A RAS cannot have more than 32 snlinks (4 when loadsharing). A snlink may only be associated with a single Remote Application Server. The valid range is 0-255.

SIGTRAN Remote Application Server List configuration is viewed using the CNRLP MMI command. After startup additional Remote Application Server Lists can be added to the config.txt file and then read into the system using the CNRAI command. Remote Application Servers Lists are removed from the config.txt file and then removed from the system using the CNRAE MMI command.

5.7.6 STN_ROUTE - SIGTRAN Route Configuration

Synopsis

This command is used to configure a SIGTRAN route to a remote SS7 destination.

Applicability

SIU, SWS, DSH

Syntax

```
STN_ROUTE:[NC=NC0],SNRT=,DPC=[,OPTIONS=0][,LABEL=];
```

Examples

```
STN_ROUTE:SNRT=,DPC=100;
STN_ROUTE:NC=NC0,SNRT=2,DPC=200;
```

Parameters

The STN_ROUTE command has the following parameters:

- **NC**

SS7 Network Context. The Network Context together with the Destination Point Code (DPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.

- **SNRT**

Logical reference for a SIGTRAN Route. The valid range is 0-4095.

- **DPC**

Specifies an Destination Point Code (DPC) value for the Remote Application Server. Only one Remote Application Server, SIGTRAN Route or C7 Route can be configured with a particular DPC within a network context.

- **OPTIONS**

This is a 16 bit value used to specify run time options:

Bit	Description
0	Route is assumed to be available.
1	Route will loadshare between all Signaling Gateways in the route.
2	The route will be designated to be the a default Route for the Network Context. The default route will be selected if no match is found in the M3UA routing tables for the DPC of a message destined for the network. If bit 0 of the STN_ROUTE flags is also set then the Default Route will become available as soon as the network connections become available. In this case the DPC in the Route serves little purpose (though must still be unique in the Routing Table). A DPC of Zero could be used. If bit 0 of the STN_ROUTE flags is not set then the Default Route will only become available when the DPC used in the configuration message becomes available. The Point Code of the Signaling Gateway through which the Route connects to the network may be used.
3-15	Reserved and should be set to zero.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

SIGTRAN Route configuration is viewed using the CNSRP MMI command and its status and measurements read using the STSRP an MSRAP MMI commands. After startup additional Remote Application Routes can be added to the config.txt file and then read into the system using the CNSRI command. Routes are removed from the config.txt file and then removed from the system using the CNSRE MMI command.

5.7.7 STN_RSGLIST - SIGTRAN Route Signaling Gateway List Configuration

Synopsis

This command attaches Signaling Gateways to a SIGTRAN Route.

Applicability

SIU, SWS, DSH

Syntax

```
STN_RSGLIST:GLID=,SNRT=,RSG=[,OPTIONS=0];
```

Examples

```
SSTN_RSGLIST:GLID=0,SNRT=1,RSG=1,OPTIONS=0x0001;
STN_RSGLIST:GLID=1,SNRT=2,RSG=1,OPTIONS=0x0001;
STN_RSGLIST:GLID=2,SNRT=3,RSG=1,OPTIONS=0x0001;
```

Parameters

The STN_RSGLIST command has the following parameters:

- **GLID**

Logical identifier for a SIGTRAN Route to Signaling Gateway relationship. The valid range is 0-6399.

- **SNRT**

Logical reference for a SIGTRAN Route. The valid range is 0-255.

- **RSG**

Remote Signaling Gateway. A Signaling Gateway can be associated with a route only once. The Signaling Gateway must have at least 1 snlink associated with it. The valid range is 0-255.

- **OPTIONS**

This is a 16 bit value used to specify run time options:

Bit 0 - When set, the Signaling Server will consider the route via the specified server to be available without waiting for a destination available (DAVA) message.

All other bits are reserved for future use.

SIGTRAN Route Gateway List configuration is viewed using the CNGLP MMI command. After startup additional Route Gateway Lists can be added to the config.txt file and then read into the system using the CNGLI command. Route Gateway Lists are removed from the config.txt file and then removed from the system using the CNGLE MMI command.

5.7.8 STN_LBIND - SIGTRAN Local Bind Configuration

Synopsis

This command associates the local application server with the Remote Application Server or Remote Signaling Gateway, identifying the route to reach the destination.

The software supports M3UA IPSP Single Ended (SE) communication; therefore, the Remote Application Server must have the same routing context as the Local Application Server. When communicating with multiple Remote Application Servers there must be additional Local Application Servers, each having a different routing context.

Applicability

SIU, SWS, DSH

Syntax

```
STN_LBIND:BIND=,LAS=,RAS=[,OPTIONS=0];
STN_LBIND:BIND=,LAS=,RSG=[,OPTIONS=0];
```

Example

```
STN_LBIND:BIND=1,LAS=1,RSG=3;
```

Parameters

The STN_LBIND command has the following parameters:

- **BIND**

Logical identifier for a binding between a Local Application Server and either a Remote Application Server or Remote Signaling Gateway. The valid range is 0-199.

- **LAS**

Logical reference for a Local Application Server. An underlying snlink may only be associated with a single LAS. The valid range is 0-199.

- **RAS**

Remote Application Server. The Remote Application Server must be associated with at least one SIGTRAN Link and cannot be bound to more than one Local Application Server. In IPSP operation the Local Application Server and Remote Application Server must be associated with same network context. The valid range is 0-255.

- **RSG**

Remote Signaling Gateway. The Remote Signaling Gateway must be associated with at least one SIGTRAN Link. The valid range is 0-255.

- **OPTIONS**

This is a 16 bit value used to specify run time options. This field is reserved for future use and should be set to 0.

SIGTRAN Binds configuration is viewed using the CNSBP MMI command. After startup additional Binds can be added to the config.txt file and then read into the system using the CNGLI command Binds are removed from the config.txt file and then removed from the system using the CNGLE MMI command.

5.7.9 SCTP_TIMER - SCTP Timer Configuration

Synopsis

The SCTP_TIMER command provides the ability to configure the SCTP protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
SCTP_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
SCTP_TIMER:TIMID=RMAX,TMSEC= 1600;
```

NC

```
<nc_id>
```

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SCTP timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

TIMID

A text identifier for the timer to be configured. It should be set to one of the following:

RMIN, RMAX, RINIT, CK, HBT, T1I, T2I, SACKD

TSEC

The timer value specified in seconds.

TMSEC

The timer value specified in milliseconds.

Any timers not explicitly configured continue will be set to the default values shown in the following table:

Mnemonic	Default	Granularity	SCTP Timeout
Rmin	200ms	1ms	Minimum RTO
Rmax	1400ms	1ms	Maximum RTO
Rinit	1000ms	1ms	Initial RTO
Ck	30000ms	1ms	Cookie lifetime
Hbt	1000ms	1ms	Time between heartbeats
T1i	3000ms	1ms	Starting timeout of an INIT chunk
T2i	3000ms	1ms	Starting timeout of a SHUTDOWN chunk
Sackd	10ms	1ms	SACK delayed Ack

The SCTP_TIMER command may also be used to modify the number times a heartbeat or data packet may be retransmitted before an association is determined to have failed. The following table provides a description of these parameter as well as indicating their default value. N.B. Increasing the number of retransmissions before failure is determined will obviously delay any corrective action that may be taken.

Mnemonic	Default	Description
RtxHb	3	The number of times a heartbeat packet may be transmitted before determining that an association has failed.
RtxData	3	The number of times a data packet may be transmitted before determining that an association has failed.

5.7.10 M2PA_TIMER - M2PA Timer Configuration

Synopsis

The M2PA_TIMER command provides the ability to configure the M2PA protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
M2PA_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
M2PA_TIMER:NC= NC1,TIMID=T7,TSEC= 1,TMSEC=500;
```

Parameters

NC

SS7 Network Context. This parameter uniquely identifies the SS7 network that the M2PA timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

TIMID

A text identifier for the timer to be configured. It should be set to one of the following:

T1, T2, T3, T4N, T4E, T6, or T7

TSEC

The timer value specified in seconds.

TMSEC

The timer value specified in milliseconds.

Any timers not explicitly configured continue will be set to the default values shown in the following table:

Mnemonic	Default	Granularity	M3UA Timeout
T1	45s	100ms	'Alignment Ready' timer value
T2	30s	100ms	'Not Aligned' timer value
T3	1.2s	100ms	'Aligned' timer value
T4N	8.2s	100ms	'Normal Proving' timer value
T4E	0.5s	100ms	'Emergency Proving' timer value
T6	5.5s	100ms	'Remote Congestion' timer value
T7	1.7s	100ms	'Excessive Delay Of Acknowledgement' timer value

5.7.11 M3UA_TIMER - M3UA Timer Configuration

Synopsis

The M3UA_TIMER command provides the ability to configure the M3UA protocol timers from the configuration file.

Applicability

SIU, SWS, DSH

Syntax

```
M3UA_TIMER:[NC=NC0],TIMID=[,TSEC=][,TMSEC=];
```

Example

```
M3UA_TIMER:NC= NC1,TIMID=TACK,TSEC=3;
```

Parameters

NC

SS7 Network Context. This parameter uniquely identifies the SS7 network that the M3UA timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

TIMID

A text identifier for the timer to be configured. It should be set to one of the following:

Tack, Tr, Tdaud, Tbeat.

TSEC

The timer value specified in seconds.

TMSEC

The timer value specified in milliseconds.

Any timers not explicitly configured continue will be set to the values shown in the following table:

Mnemonic	Default	Granularity	M2PA Timeout
Tack	2s	100ms	Peer response timeout
Tr	1s	100ms	Recovery timer for inactive ASPs
Tdaud	30s	1s	DAUD generation timer
Tbeat	30s	1s	M3UA heartbeat timer

5.8 Message Router Configuration Commands

The ISUP commands include:

- "MRF_OG - Message Router Origin Configuration"
- "MRF_DE - Message Router Destination Configuration"
- "MRF_RK - Message Router Routing Key Configuration"
- "MRF_CP - Message Router Custom Profile Configuration"
- "MRF_CE - Message Router Concerned Entity"

5.8.1 MRF_OG - Message Router Origin Configuration

Synopsis

The MRF_OG command initiates a Message Router Origin. An Origin identifies the point from which an incoming message is received. An Origin is specified by the DOMAIN (Application Server, Network or User Part), Network Context and Service Indicator. Each origin must be assigned a Routing Key table identifier to indicate which set of Routing Keys should be applied.

Optionally a Custom Profile may be assigned for manipulating parameters in the Routing Label. When a Custom Profile is assigned to an Origin the parameter manipulation occurs before the parameters are compared with the Routing Key.

The Origin has its own unique identifier (OGID) and can optionally be assigned a text based label (LABEL) to assist with identification.

If the DOMAIN is NETWORK or AS then all traffic for the associated Service Indicator will be processed by the Message Router rather than being passed directly to ISUP or SCCP (or a user module on a host configured by the MTP_USER_PART command).

If the DOMAIN is UPART, then all outgoing messages from the User Part (e.g., ISUP or SCCP) will be processed by the Message Router rather than being transmitted directly to the network.

Note: When a Message Router Origin for a particular Network Context is configured in the NETWORK domain Bit 0, Bit 17 and Bit 22 of the options parameter for any associated MTP_CONFIG and MTP_NC_CONFIG commands will automatically be set. These bits controls how received Route Set Test, Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the MTP local point code are processed and are set to allow the Message Router to correctly processing these messages for the domains and Network Contexts under its control.

Note: When a Message Router Origin for a particular Network Context is configured in the UPART domain with a service indicator of 3 and a user configures SCCP on the Signaling Server in that Network Context bit 2 of the <options2> parameter in the SCCP_CONFIG and SCCP_NC_CONFIG commands will automatically be set. Setting this bit allows the Message Routing functionality to understand the point code format of messages transmitted by SCCP.

Syntax

```
MROGI:[NC=NC0],OGID=,DOMAIN=,RKTAB=,SI=[,OPC=ANY][,CP=NONE][,LABEL=];
```

Example

```
MRF_OG:OGID=1,DOMAIN=NETWORK,SI=5,RKTAB=1;
MRF_OG:NC=NC0,OGID=2,DOMAIN=AS,SI=5,RKTAB=1,CP=NONE;
MRF_OG:OGID=3,NC=NC0,DOMAIN=USER,SI=3,RKTAB=2,CP=1;
```

Parameters

NC

SS7 Network Context. This parameter identifies the SS7 Network Context associated with the Origin. Supported values are: NC0, NC1, NC2 or NC3. When the parameter omitted, a value of NC0 is assumed.

OGID

Logical identifier for the Origin. A number in the range 0-4095.

DOMAIN

The domain a message is being received from. A domain may be either NETWORK (either the MTP network or M3UA when connected to a Signaling Gateway), User Part (UPART) or AS (M3UA when connected to an Application Server).

SI

Service Indicator in the range 0-15. Received messages containing the configured SI will be considered to match the Origin. If required a different Origin may be configured for each SI.

OPC

Originating Point Code. When set to a value other than the default of ANY received messages containing the OPC will be considered to match the aspect of the origin.

RKTAB

Logical Identifier for the table of Routing Keys associated with this Origin. A number in the range 0-49.

CP

Logical identifier for a custom profile that may be used to modify the routing label AFTER the routing table has been determined for routing. If the parameter is omitted or set to NONE then there is no custom profile present. The parameter is optional and will default to NONE.

LABEL

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

5.8.2 MRF_DE - Message Router Destination Configuration

Synopsis

The MRF_DE command initiates a Message Route Destination. Destinations can be used to route traffic to a Remote Application Server in the AS DOMAIN, to the SS7 Network in the NETWORK DOMAIN or to a local user application in the UPART DOMAIN where the destination module id will be determined by Network Context and Service Indicator in the message to be transmitted.

The command may also router traffic to a DOMAIN of PARTNER. Traffic routed to a partner Signaling Server will be considered on the receiving signaling server to be either from the original NETWORK, AS or USER domains of the transmitting Signaling Server.

A Destination is selected as a result of a Routing Key match. The hunting algorithm use to search through the entries in the destination table is specified by the HUNT parameter in the Routing Key.

If the Destination table cannot find an available Remote Application Server in the AS DOMAIN or Destination Point Code in the NETWORK DOMAIN the message router will pass the message onto the partner Signaling Server, if available or discard the message if the partner Signaling Server is not available or had previously forwarded the message.

A Custom Profile can be set to modify the routing label.

Syntax

```
MRF_DE:[NC=NC0],DESTID=,DEST=,DESTSEQ=,DOMAIN=[,RAS=][,CP=][,DPC=][,LABEL=];
```

Example

```
MRF_DE:DESTID=1,DEST=1,DESTSEQ=1,DOMAIN=AS ,RAS=1;
MRF_DE:DESTID=2,DEST=2,DESTSEQ=2,DOMAIN=NETWORK;
MRF_DE:DESTID=3,DEST=3,DESTSEQ=3,DOMAIN=UPART,RAS=NONE,CP=NONE;
```

Parameters

DESTID

Logical identifier for the Destination in the range 0-4095.

DEST

The Destination table ID (as specified in a Routing Key) in the range 0-4095.

DESTSEQ

The sequence number of this Destination within the Destination table in the range 0-31.

DOMAIN

The destination domain for a message. A domain may be either NETWORK (either the a MTP network or M3UA when acting as an ASP), User Part (UPART), AS (M3UA when acting as a Signaling Gateway) or PARTNER (when routing to the partner Message Router). If the domain is set to AS the associated Remote Application Server is determined by the RAS parameter.

NC

SS7 Network Context. This parameter identifies the SS7 network messages will be sent to. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.

RAS

The destination Remote Application Server to which messages will be sent. This parameter is used only when DOMAIN=AS. The Remote Application Server associated with a Destination must be configured to be acting as a Local Signaling Gateway.

CP

Logical identifier for a custom profile that may be used to modify the routing label AFTER the row in the destination table has been selected for routing. If the parameter is set to NONE then there is no custom profile present. The parameter is optional and will default to NONE.

DPC

Destination Point Code. If present, the status of the configured DPC will be checked and the table row will only be selected if the DPC is available. If available, this DPC will be copied into the routing label of the message.

LABEL

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

5.8.3 MRF_RK - Message Router Routing Key Configuration

Synopsis

The MRF_RK command initiates a Message Router Routing Key. Routing Keys are used to filter messages by matching the individual Routing Label fields from the received message with those contained in the Routing Key to determine the appropriate Destination.

Each Routing Key belongs to a table (identified by the RKTAB parameter) which must be specified for each Origin that needs to use the Routing Key.

Syntax

```
MRF_RK: RKI=,RKTAB=,[OPC=,][DPC=,][SI=,][NI=,][CIC_RANGE=,][HUNT=,]DEST=,[CP=,][LABEL=,]
```

Example

```
MRF_RK:RKI=1,RKTAB=1,SI=3,DEST=1;
MRF_RK:RKI=2,RKTAB=1,OPC=ANY,DPC=ANY,SI=5,,HUNT=FIRST,DEST=1;
MRF_RK:RKI=2,RKTAB=2,SI=3,DEST=2,LABEL=London;
MRF_RK:RKI=4,RKTAB=2,OPC=43434,DPC=44343,SI=5,CIC_RANGE=1-2000, HUNT=BALANCE,DEST=1;
```

Parameters

RKI

A Routing Key Index in the range 0-4095 used to uniquely identify a particular Routing Key.

RKTAB

Logical Identifier of the Routing Key table in the range 0-49.

OPC

The OPC specified should match the one in message before the Routing Key entry is considered a match. If OPC is set to ANY then any OPC is considered a match. The parameter is optional and defaults to ANY.

DPC

The DPC specified should match the one in message before the Routing Key entry is considered a match. If DPC is set to ANY then any OPC is considered a match. The parameter is optional and defaults to ANY.

NI

The Network Indicator specified should match the one in message before the Routing Key entry is considered a match. The parameter is optional and defaults to ANY.

SI

The Service Indicator specified should match the one in message before the Routing Key entry is considered a match. The parameter is optional and defaults to ANY.

CIC_RANGE

The CIC range specifies a subset of ISUP/BICC CICs that a message should contain before the Routing Key is considered a match. The CIC range is a compound parameter of the form <base-range> where <base> is the base (or first) CIC in the range and <range> is the number of CICs in the range. If not specified, CIC_RANGE defaults to ANY.

HUNT

The Hunting Method for the Destination determined by the Routing Key. The parameter is optional and defaults to FIRST. Possible values are:

- FIRST – The first available Destination will be selected.
- CIRCULAR – The next available Destination will be selected from the Destination table in a round robin manner each time a new message is routed.
- BALANCE – Currently only valid for SI=5 or 13. Each time a new call arrives, the Destination will be selected from the Destination table in a round robin manner. Subsequent messages for the same call/circuit will be routed to the same Destination.
- SHARE1 - A destination from a destination table will be selected based on the SLS field in the received message. If the destination is not available the next available destination will be selected based on the SLS and the number of remaining destinations.

DEST

The Destination table determined by the Routing Key

CP

Logical identifier for a custom profile that may be used to modify the routing label AFTER the routing key has been matched and the destination table has been determined for routing. If the parameter is set to NONE then there is no custom profile present. The parameter is optional and defaults to NONE.

LABEL

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

5.8.4 MRF_CP - Message Router Custom Profile Configuration

Synopsis

The MRF_CP command initiates a Custom Profile which can be used by an Origin, Routing Key or Destination to modify the routing label of messages passing through the Message Router.

Syntax

```
MRF_CP:CP=,[OPC=,][DPC=,][NI=,][SI=,][LABEL=,];
```

Example

```
MRF_CP:CP= 1,OPC=1423,DPC=2322;
```

Parameters

CP

Logical identifier for the custom profile in the range 0-4095.

OPC

If the value is not ‘NONE’ then the OPC specified will replaced the OPC in the message the profile is being applied to. This parameter is optional and defaults to NONE.

DPC

If the value is not ‘NONE’ then the DPC specified will replaced the DPC in the message the profile is being applied to. This parameter is optional and defaults to NONE.

NI

If the value is not ‘NONE’ then the Network Indicator specified will replaced the Network Indicator in the message the profile is being applied to. This parameter is optional and defaults to NONE.

SI

If the value is not ‘NONE’ then the Service Indicator specified will replaced the Service Indicator in the message the profile is being applied to. This parameter is optional and defaults to NONE.

LABEL

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

5.8.5 MRF_CE - Message Router Concerned Entity

Synopsis

The MRF_CE command defines a Concerned Entity defines entities that need to be notified in the event of the accessibility of the DPC changing.

Syntax

```
MRF_CE:[NC=,]CONCID=,DPC=,CONC_DOMAIN=,[CONC_NC=,]CONC_ENT=,[ALIAS=,];
```

Example

```
MRF_CE:CONCID=1,DPC=2322,CONC_DOMAIN=NETWORK,CONC_ENT=256;
MRF_CE:NC=NC0,CONCID=2,DPC=653,CONC_DOMAIN=AS,CONC_NC=NC0,CONC_ENT=1;
```

Parameters

NC

SS7 Network Context. This parameter identifies the SS7 network in which the Destination Point Code exists. Supported values are: NC0, NC1, NC2 or NC3. Defaults to NC0 if not specified.

CONCID

Logical identifier for the concerned relationship in the range 0-4095.

DPC

The Destination Point Code who's status the concerned point code needs to be informed about. If set to ANY the Concerned Point Code will be concerned about all point codes in the network context. If explicitly configured, the DPC must have already been configured as one of the following:

- A DPC associated with an MTP Route,
- A DPC associated with a Sigtran Route,
- A DPC associated with a Sigtran Remote Application Server,
- An OPC associated with an MTP Link Set,
- or an OPC associated with a Sigtran Local Application Server.

CONC_DOMAIN

The Concerned Domain that is to be notified of the change in status. Possible values are:

- AS
  The Concerned Entity is an Application Server which has been configured as a Sigtran Remote Application Server.
- NETWORK
  The Concerned Entity is an Adjacent Point Code in the NETWORK domain.
- UPART
  The Concerned Entity is a User Part (identified by Service Indicator). The User Part associated with the Service Indicator should already be specified on a routing origin command.

CONC_NC

The Network Context in which the Concerned Entity exists. For ASP entities it must be the same NC as that used on the ASLINK. If not specified, CONC_NC defaults to the same value as NC.

CONC_ENT

The Concerned Entity which is a reference to a specific entity in the Concerned Domain which will be informed of the change in status of the DPC.

If CONC_DOMAIN=NETWORK then CONC_ENT is the adjacent point code that needs to be notified. If set to ANY then all point codes in the CONC_NC will be informed.

If CONC_DOMAIN=AS then CONC_ENT is the Remote Application Server (RAS) that is concerned about the status of the DPC. If set to ANY then all Remote Application Servers in the CONC_NC will be informed.

If CONC_DOMAIN=UPART then CONC_ENT is the Service Indicator (SI).

ALIAS

An Alias for the Destination Point Code that will be presented to the affected entity as the Point Code that has changed state. NONE or Number from 0 to 16777215. An Alias Point Code may be used for example when a change in state for a particular point code in one network should be represented as a change in state for a point code that exists in a different network. If an Alias point code is specified the DPC must be explicitly defined. ALIAS defaults to NONE if not specified.

5.9 ISUP Configuration Commands

The ISUP commands include:

- ISUP_CONFIG - ISUP Configuration
- ISUP_CFG_CCTGRP - ISUP Circuit Group Configuration
- ISUP_TIMER - ISUP Timer Configuration

5.9.1 ISUP_CONFIG - ISUP Configuration

Synopsis

The ISUP_CONFIG command supplies the configuration parameters that specify the operating environment of the ISUP protocol. This command should only be used if the ISUP software has been licensed and configured on the Signaling Server.

Applicability

SIU

Syntax

```
ISUP_CONFIG <OPC> <SSF> <USER_ID> <OPTIONS> <NUM_CGRPS> <NUM_CCTS> <MAXSIF>
```

Example

```
ISUP_CONFIG 2 0x8 0x1d 0x0434 128 4096
```

Parameters

The ISUP_CONFIG command includes the following parameters:

- **OPC**

The default local point code of the Signaling Server for ISUP.

- **SSF**

The sub-service field value that ISUP uses when exchanging messages with the MTP. This must always be set so that the Network Indicator bits (the two most significant bits of the 4-bit ssf value) match those set in the MTP_LINKSET command.

- **USER_ID**

The unique module identifier (module_id) of the application running on the host that uses the ISUP module. The ISUP module sends all receive indications to this module ID. This must be in the range 0x0d, 0x1d, 0x2d to 0xfd, where 0xnd is defined as APPn_TASK_ID.

- **OPTIONS**

A 16-bit value that contains run time options for the operation of the ISUP protocol:

— Bit 0 should always be set to 0.

— Bit 15: For the purposes of the measurement MMI command MSCGP when not set the point of a call being 'answered' is determined by generation or reception of either an Answer message or a Connect message. When set the 'answer' point is considered to occur when an address complete is generated or received. Setting the bit is more useful for certain types of application which use the time between Address Complete and Answer to play tones or announcements.

— The remaining bits are as defined for the **options** parameter defined in the Configure Request section of the *ISUP Programmer's Manual*.

- **NUM_GRPS**

Specifies the number of circuit groups to be used by ISUP. This parameter may be in the range 1 to 2,048. If this parameter is not specified, the Signaling Server allows 8 circuit groups.

- **NUM_CCTS**

Specifies the number of circuits to be used by ISUP. This parameter may be in the range 1 to 65,535.

Note: ISUP allows the configuration of **cid** values in the range 0 to <num_ccts> – 1.

- **MAXSIF**

Specifies the maximum size of a message transmitted by the ISUP module on the Signaling Server. For ISUP operation, this should be 272 octets. For BICC operating above M3UA, a user may specify up to 544 octets to allow larger messages to be transmitted without the need for segmentation. Support for sif values above 272 is application dependent and depends on the maximum size a receiving switch can process.

5.9.2 ISUP_CFG_CCTGRP - ISUP Circuit Group Configuration

Synopsis

The ISUP_CFG_CCTGRP command configures an ISUP circuit group. Normally, all circuits on a single T1 or E1 interface would be assigned to the same circuit group. A single command enables the operating parameters for all the circuits in the group to be specified. Circuit groups are described fully in the *ISUP Programmer's Manual*.

Applicability

SIU

Syntax

```
ISUP_CFG_CCTGRP [,<NC>] <GID> <DPC> <BCIC> <BCID> <CIC_MASK> <OPTIONS> <USER_HOST> <USER_ID> <OPC>
<SSF> <VARIANT> <OPTIONS2>
```

Example

```
ISUP_CFG_CCTGRP 0 3 1 1 0x7fff7fff 0x0003 0 0x1d 1 0x8 4 0
ISUP_CFG_CCTGRP NC0 0 3 1 1 0x7fff7fff 0x0003 0 0x1d 1 0x8 4 0
```

Parameters

The ISUP_CFG_CCTGRP command includes the following parameters:

- **NC**

SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.

- **GID**

The unique logical identifier of the circuit group within the Signaling Server. This parameter should be in the range 0 to one less than the maximum number of circuit groups that ISUP processes, set by the ISUP_CONFIG **<num_grps>** parameter.

- **DPC**

The Destination Point Code (DPC) at which the voice circuits in this group terminate.

- **BCIC**

The Circuit Identification Code (CIC) that is allocated to the first circuit in the circuit group.

- **BCID**

The logical ID for the first circuit in the circuit group. It must lie in the range 0 to one less than the number of circuits supported.

- **CIC_MASK**

Each circuit group may contain up to 32 circuits. Setting bits in <cic_mask> identifies the circuits allocated to the circuit group. The least significant bit (bit 0) corresponds to the first CIC and must always be set. Bit n in the <cic_mask> corresponds to circuit identification code = (<base_cic> + n) and circuit identifier = (<base_cid> + n). If the bit is not set, then this CIC and CID can instead be allocated to a different circuit group.

Note: A single circuit group may not span more than 32 CICs.

- **OPTIONS**

A 32-bit value where each bit represents a run-time option for the circuit group.

— The meaning of the lower 16 bits are as defined in the **options** parameter described in the Configure Circuit Group Request section of the *ISUP Programmer's Manual*.

— The meaning of the upper 16 bits are as defined in the **ext_options** parameter described in the Configure Circuit Group Request section of the *ISUP Programmer's Manual*.

- **USER_HOST**

The logical identifier of the host to which receive indications and circuit group supervision indications for this group are to be sent.

- **USER_ID**

Specifies a user application module ID for this circuit group. This overwrites the user_id specified in the ISUP_CONFIG command.

- **OPC**

Specifies an Originating Point Code (OPC) value for this group and overwrites the default local signaling point code specified with the ISUP_CONFIG command. This parameter enables the Signaling Server to behave as a different local point code for each circuit group; such a configuration is used when connecting to multiple networks. This also facilitates the loop-back of ISUP routes locally for local loop-back testing.

- **SSF**

Specifies a sub-service field value for this circuit group. This overwrites the ssf specified using the ISUP_CONFIG command.

- **VARIANT**

An 8-bit field that is mapped directly to the variant field in the ISUP Circuit Group Configuration message. The following table details the current variants:

Variant Value	Variant Description
0	Blue Book ISUP
1	1992 ISUP
2	ANSI ISUP
3	German ISUP
4	UK ISUP
5	Japanese TTC ISUP
6	ANSI RLT ISUP
7	ITU RLT ISUP
8	ANSI 95 ISUP
9	Italian ISUP
10	SSURF - French ISUP
11	China ISUP
12	ISUP 2000/ETSI V4
13	BICC

- **OPTIONS2**

A 32-bit field that is mapped directly to the ext_1_options field in the ISUP Circuit Group Configuration message described in the *ISUP Programmer's Manual*. Currently the following bits are significant:

Bit	Description
0	Add ST digits to Called party number
1	Select 16-bit Point Code format (for Japanese operation)
2	Do not send REL on T33 expiry (waiting for INF)
3	Usr-to-usr srvc does not have to be requested to use uuinf param
8	Any Calling Party Clearing Indication received is passed transparently to the user application
9	Generate periodic heartbeat messages towards the user_id configured for the circuit group. If no acknowledgement is received for the heartbeat, then blocking of circuits is performed.
10	When ISUP must release the call to the user, a Location value of "LPN, private network serving the local user (1)" will be indicated in the Cause parameter. Otherwise, a Location value of "RPN, private network serving the remote user (5)" will be indicated.
22	If set and ISUP has been configured for 24 bit point codes ISUP will set the SLS to the 8 least significant bits of the CIC otherwise it will set the SLS to 5 bits.

Circuit Group configuration is viewed using the CNCGP MMI command and its status and measurements read using the STCGP an MSCGP MMI commands. After startup additional Groups can be added to the config.txt file and then read into the system using the CNCGI command. Groups are removed from the config.txt file and then removed from the system using the CNCGE MMI command.

5.9.3 ISUP_TIMER - ISUP Timer Configuration

Synopsis

The ISUP_TIMER command provides the ability to configure the ISUP protocol timers from the config.txt file.

Applicability

SIU

Syntax

```
ISUP_TIMER <TIMTAB> <TIMID> <TVAL>
```

Example

```
ISUP_TIMER 0 t4 550
```

Parameters

The ISUP_TIMER command includes the following parameters:

- **TIMTAB**

Set to 0 to configure ISUP timers. Set to 1 to configure BICC timers. All other values are reserved for future use.

- **TIMID**

The text identifier for the timer to be configured. It should be set to one of the following values: T1,T2, T3, T5, T6, T7, T8, T9, T10, T11, T12, T13, T14, T15, T16, T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29, T30, T33, T34, T35, T36, T38, T103 or T104.

- **TVAL**

The timer value in seconds, except T29 and T30 that are in multiples of tenths of a second (100ms). Any timers not configured continue to be set to the values shown in the following table.

ISUP Timer	Default Value (seconds)	ISUP Timer	Default Value (seconds)	ISUP Timer	Default Value (seconds)
T1	10	T15	60	T27	240
T2	180	T16	10	T28	10
T3	180	T17	60	T29	5 tenths
T5	60	T18	10	T30	80 tenths
T6	180	T19	60	T33	14
T7	25	T20	10	T34	3
T8	13	T21	60	T35	20
T9	45	T22	10	T36	13
T10	5	T23	60	T38	150
T12	10	T24	2	T39	10
T13	60	T25	5	T103	20
T14	10	T26	120	T104	3

Note: The SIU does not perform checks on ISUP timer values.

5.10 SCCP Configuration Commands

The SCCP configuration commands include:

- SCCP_CONFIG - SCCP Configuration
- SCCP_LOAD_SHARE_TABLE - SCCP Load Share Table
- SCCP_LOAD_SHARE_DPC - SCCP Load Shared DPCs

- SCCP_GTT - Global Title Translation
- SCCP_GTT_ADDRESS - Global Title Translation Address
- SCCP_GTT_PATTERN - Global Title Translation Pattern
- SCCP_RSP - SCCP Remote Signaling Points
- SCCP_LSS - SCCP Local Sub-Systems
- SCCP_RSS - SCCP Remote Sub-Systems
- SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration

5.10.1 SCCP_CONFIG - SCCP Configuration

Synopsis

The SCCP_ CONFIG command defines the global configuration parameters for SCCP either when existing in a single network or when existing in multiple Network Contexts. The SCCP_CONFIG command is used to configure and activate the SCCP and TCAP protocols on the Signaling Server. This command should only be used if the SCCP and TCAP software has been licensed and configured on the Signaling Server.

A SCCP_CONFIG command for NC0 must be configured prior to configuring SCCP_CONFIG commands for other Network Contexts.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_CONFIG:[NC=NC0],OPC=,SSF=[,OPTIONS=0][,OPTIONS2=0x00000001];
```

Example

```
SCCP_CONFIG:NC=NC0,OPC=123;
```

Parameters

The SCCP_CONFIG command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network for which SCCP is being configured. Supported values are: NC1, NC2 and NC3.

- **OPC**

The local point code of the Signaling Server.

- **SSF**

The sub-service field value that SCCP uses when exchanging messages with the MTP. This must always be set so that the Network Indicator bits (the two most significant bits of the 4-bit ssf value) match those set in the MTP_LINKSET command.

- **OPTIONS**

A 32-bit value containing run-time options for the operation of the SCCP module. The 16 most significant bits provide ext_options, as defined in the *SCCP Programmer's Manual*.

— Bit 0 should always be set to 0.

— Bit 1 should always be set to 1.

— Bit 20 should be set to 1 when using SCCP in conjunction with DTS and dual resilient configuration.

— The meaning of the remaining bits are as defined for the **options** parameter described in the Configuration Request section of the *SCCP Programmer's Manual*.

- **OPTIONS2**

A 32-bit field that is mapped directly to the ext_1_options field in the SCCP module Configuration message described in the *SCCP Programmer's Manual*. Currently the following bits are significant.

— Bit 0: Allows the selection of automatic or local subsystem generated "user in service" indications. When set it a "user in service" SCP_MSG_SCMG_REQ message is automatically send to SCCP for all configured local subsystems. When not set local subsystems should send the SCP_MSG_SCMG_REQ message manually when they are available.

— Bit 1: When set automatic generation of UDTS messages by SCCP is disabled.

Other bits should be set to 0.

Note: When a Message Router Origin for a particular Network Context is configured in the UPART domain with a service indicator of 3 bit 2 of the <options2> parameter in the SCCP_CONFIG, commands will automatically be set for the particular Network Context. Setting this bit allows the Message Routing functionality to understand the point code format of messages transmitted by SCCP.

5.10.2 SCCP_LOAD_SHARE_TABLE - SCCP Load Share Table

The SCCP_LOAD_SHARE_TABLE command is a new configuration command and is defined as follows:

Synopsis

The SCCP_LOAD_SHARE_TABLE statement initiates a Global Title Load Share table (GLST). Once defined the SCCP_LOAD_SHARE_DPC command can be used to associate Destination Point Codes with this Global Title Load Share table (GLST). The GLST can then be assigned to a SCCP address using the DPC parameter on the SCCP_GTT_ADDRESS command.

Syntax

```
SCCP_LOAD_SHARE_TABLE:[NC=NC0],LST=[,OPTIONS=0];
```

Example

```
SCCP_LOAD_SHARE_TABLE:NC=NC0,LST=LST=5,OPTIONS=0x00000001;
SCCP_LOAD_SHARE_TABLENC1LST-70x00000003
```

Parameters

- **NC**

SS7 Network Context. This parameter identifies the SS7 network in which the Destination Point Code exists. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.

- **LST**

logical id of the LST instance in the range 0 -255. The value is prefixed with the string 'LST' so that when it is assigned to an SCCP_GTT_ADDRESS it can be distinguished from an individual Point Code.

- **OPTIONS**

- Bit 0 - If set, the availability test for each GLST entry requires that both the Point Code and the Sub-system are available. If not set, only the GLST Point Code is tested for availability.
- Bit 1 - When set to 0 to Point Code selection can be made using the Signaling Link Selection (SLS) value for messages received from the network, or Sequence Control (SEQ_CTRL) parameter for messages received from the User Part.

  When set to 1 messages will be distributed across the point codes on a Round Robin basis ignoring SLS values.
- Bits 2-31 - Reserved for future used. Should be set to 0.

5.10.3 SCCP_LOAD_SHARE_DPC - SCCP Load Shared DPCs

The SCCP_LOAD_SHARE_DPC command is a new configuration command and is defined as follows:

Synopsis

The SCCP_LOAD_SHARE_DPC statement associates a Destination Point Code with a Global Title Load Share table defined by the SCCP_LOAD_SHARE_TABLE command. The Global Title Load Share table can then be assigned to a SCCP address using the SCCP_GTT_ADDRESS DPC parameter on the command.

Syntax

```
SCCP_LOAD_SHARE_DPC:LSTSEQ=,DPC=;
```

Example

```
SCCP_LOAD_SHARE_DPC:LSTSEQ=LST=5-0,DPC=2222;
SCCP_LOAD_SHARE_DPC:LSTSEQ=LST=5-1,DPC=2223;
SCCP_LOAD_SHARE_DPC:LSTSEQ=LST=6-1,DPC=1011;
SCCP_LOAD_SHARE_DPC:LSTSEQ=LST=6-2,DPC=1014;
SCCP_LOAD_SHARE_DPC:LSTSEQ=LST=6-3,DPC=1015;
```

Parameters

- **LSTSEQ**

The Loadshare table index sequence number identifies the position of a Destination Point Code entry in a loadshare table. It is made up of a loadshare table ID (LST-x) with the sequence number as a suffix (e.g., LST-0-0).

Note: When assigning sequence numbers to a loadshare table they must start at 0 and increment without gaps in the sequence.

- **DPC**

The remote signaling point code associated with the load share table.

Note: To achieve % load balancing, the same <dpc> can be associated with a GLST table more than once.

5.10.4 SCCP_GTT - Global Title Translations

Synopsis

The SCCP_GTT statement adds a translation to the SCCP global title translation table. This command must be specified after the SCCP_GTT_PATTERN and SCCP_GTT_ADDRESS commands. Guidelines for configuring GTT can be found in section Section 7.15, “GTT Configuration” on page 393.

Note: The pattern, mask, primary and backup addresses referenced by this command must have an identical number of sections.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_GTT:GTPID=5,GTT_MASK= R-/K,PRI_GTAID=9;
```

Example

```
SCCP_GTT:[NC=NC0],GTPID=,GTT_MASK=,PRI_GTAID=[,SEC_GTAID=][,GTTSRC=ANY][,BAK_DUAL=N][,OPTIONS=0][,RIID
=0];
```

Parameters

- **NC**

SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2, or NC3.

- **GTPID**

Identifies the pattern specified by the SCCP_GTT_PATTERN command. This value is also used to index the translation within the SCCP module.

- **GTT_MASK**

This is an expression detailing the operation to be applied to each section of the global title pattern. The format is exactly one operation per section and must contain exactly the same number of sections as the <gtai_pattern> parameter of the associated SCCP_GTT_PATTERN command and the <gtai_replacement> parameter of the associated SCCP_GTT_ADDRESS command.

The mask can contain the following:

Mnemonic	Function
-	Padding (ignored).
/	Separator used to split the mask into sections.
K or KEEP	The digits in the corresponding section of the global title address information undergoing translation will be preserved.
R or REPLACE	The digits in the corresponding section of the global title address information will be deleted and the digits in the corresponding section of the primary or backup address will be inserted in their place.

- **PRI_GTAID**

Identifies the SCCP_GTT_ADDRESS command the use as the primary translation.

- **SEC_GTAID**

Identifies the SCCP_GTT_ADDRESS command the use as the secondary (backup) translation.

- **GTTSRC**

Identifier the source to which the Global Title Translation applies. When GTTSRC=LOCAL, the command only applies for messages generated by a local sub-system (i.e., outgoing messages). When GTTSRC=REMOTE the command only applies to messages passed up to SCCP from the network (i.e., incoming messages). If GTTSRC=ANY (or the parameter is omitted), the command applies to all messages.

- **BAK_DUAL**

When set to Y, this causes any SCCP messages that match the GTT pattern, but cannot be routed due to a network failure, to be passed to SCCP on the partner unit so that it can reattempt routing.

- **OPTIONS**

- **RIID Routing Indicator ID**

Reserved for future use.

Global Title Translation configuration is viewed using the CNGTP MMI command. Global Titles can be added to the config.txt file and then read into the system using the CNGTI command. Global Titles are removed from the config.txt file and then removed from the system using the CNGTE MMI command.

5.10.5 SCCP_GTT_ADDRESS - Global Title Translation Address

Synopsis

The SCCP_GTT_ADDRESS command defines the global title to be used as the primary or backup destination of a translation. This command must be specified after the SCCP_GTT_PATTERN command. The global title address information of this command is combined with the global title being translated by examining the mask provided in the SCCP_GTT command.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_GTT_ADDRESS:[NC=NC0],GTAID=,AI=[,GTT_SPC=0][,SSN=0],GT=[,GTAI_REPLACEMENT=];
```

Example

```
SCCP_GTT_ADDRESS:GTAID=9,AI=0x11,GTT_SPC=0x1234,GT=0x1104,GTAI_REPLACEMENT=0-/-;
```

Parameters

- **NC**

SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2, or NC3.

- **GTAID**

A unique ID identifying the address. Values in the range 0 - 1023 are valid. A maximum of 256 address_id's may be defined within any or each Network Context.

- **AI**

The Address Indicator octet is formatted according to the point-code format specified in the SCCP_CONFIG <options> parameter and indicates which elements of addressing are present in the called party address pattern being defined. Bit usage for this parameter differs between the ITU (Q.713) and ANSI (T1.112) specifications.

For ITU, the parameter is defined as:

— Bit 8 - Reserved for national use

— Bit 7 - Routing indicator - 0:Route on GT, 1:Route on SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

0000	No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix)
0001	Global title includes Nature of Address Indicator (NAI) only. The <global_title> parameter (see below) should be a single hexadecimal octet (prefix 0x followed by two hexadecimal digits), the octet value being the NAI.

0010	Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT.
0011	Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet.
0100	Global title includes TT, NP, ES and NAI. The <global_title> parameter should be three hexadecimal octets (prefix 0x followed by six hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet and the NAI in the third octet.

Other values are undefined spares or reserved.

— Bit 2 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

— Bit 1 - PC Indicator. A 1 indicates that Point Code is used in addressing.

For ANSI the parameter is defined as:

— Bit 8 - Designated for national use. 0 indicates that the address is international and 1 indicates that the address is national.

— Bit 7 - Routing indicator -
0: Route on GT
1: Route on DPC and SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

0000	No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix)
0001	Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet.
0010	Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT.

Other values are undefined spares or reserved.

— Bit 2 - PC Indicator. A 1 indicates that Point Code is used in addressing.

— Bit 1 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

- **GTT_SPC**

The point code. This is ignored if bit 0 of <addr_indicator> is not set.

- **SSN**

The subsystem number. This is ignored if bit 1 of <addr_indicator> is not set.

- **GT**

The global title, excluding the global title address information, specified as a string of hexadecimal octets starting with 0x except when the <addr_indicator> indicates that no GT is present, when a value of 0 (zero) should be used.

- **GTAI_REPLACEMENT**

The global title address information to translate to, specified as a string of hexadecimal digits (digit 0xe is reserved) in left-to-right order (i.e., the pairs of digits are *not* swapped as would be the case for a BCD string).

In addition to hexadecimal digits, this string can contain the following characters:

Character	Function
-	Padding (ignored).
/	Separator used to split the pattern into sections. Each section can be processed differently, as specified by the <mask> parameter in the SCP_GTT command.

Global Title Address configuration is viewed using the CNGAP MMI command. Global Title Addresses can be added to the config.txt file and then read into the system using the CNGAI command. Global Title Addresses are removed from the config.txt file and then removed from the system using the CNGAE MMI command.

5.10.6 SCCP_GTT_PATTERN - Global Title Translation Pattern

Synopsis

The SCCP_GTT_PATTERN command defines the received global title pattern to be matched for a global title translation.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_GTT_PATTERN:[NC=NC0],GTPID=,AI=[,SPC=0][,SSN=0],GT=[,GTAI_PATTERN=];
```

Example

```
SCCP_GTT_PATTERN:GTPID=5,AI=0x10,GT=0x1104,GTAI_PATTERN=44/+;
```

Parameters

- **NC**

SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2 or NC3.

- **GTPID**

A unique ID identifying the pattern. Values in the range 0 - 1023 are valid. A maximum of 256 pattern_id's may be defined within any or each Network Context.

- **AI**

The Address Indicator octet is formatted according to the point-code format specified in the SCCP_CONFIG <options> parameter and indicates which elements of addressing are present in the called party address pattern being defined. Bit usage for this parameter differs between the ITU (Q.713) and ANSI (T1.112) specifications. For ITU, the parameter is defined as:

— Bit 8 - Reserved for national use

— Bit 7 - Routing indicator - 0:Route on GT, 1:Route on SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

0000	No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix)
0001	Global title includes Nature of Address Indicator (NAI) only. The <global_title> parameter (see below) should be a single hexadecimal octet (prefix 0x followed by two hexadecimal digits), the octet value being the NAI.
0010	Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT.
0011	Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet.
0100	Global title includes TT, NP, ES and NAI. The <global_title> parameter should be three hexadecimal octets (prefix 0x followed by six hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet and the NAI in the third octet.

Other values are undefined spares or reserved.

— Bit 2 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

— Bit 1 - PC Indicator. A 1 indicates that Point Code is used in addressing.

For ANSI the parameter is defined as:

— Bit 8 - Designated for national use. 0 indicates that the address is international and 1 indicates that the address is national.

— Bit 7 - Routing indicator
0: Route on GT
1: Route on DPC and SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

0000	No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix)
0001	Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet.
0010	Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT.

Other values are undefined spares or reserved.

— Bit 2 - PC Indicator. A 1 indicates that Point Code is used in addressing.

— Bit 1 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

- **SPC**

The point code. This is ignored if bit 0 of <addr_indicator> is not set.

- **SSN**

The subsystem number. This is ignored if bit 1 of <addr_indicator> is not set.

- **GT**

The global title, excluding the global title address information, specified as a string of hexadecimal octets starting with 0x except when the <addr_indicator> (see above) indicates that no GT is present, when a value of 0 (zero) should be used.

- **GTAI_PATTERN**

The pattern of global title address information to match, specified as a string of hexadecimal digits (digit 0xe is reserved) in left-to-right order (i.e., the pairs of digits are not swapped as would be the case for a BCD string).

As well as hexadecimal digits, this string can contain the following characters:

Character	Function
-	Padding (ignored).
+	Wildcard - matches any number of digits
?	Wildcard - matches exactly one digit.
/	Separator used to split the pattern into sections. Each section can be processed differently, as specified by the <mask> parameter in the SCP_GTT command.
NOTE: The "+" wildcard is not "greedy". It matches the shortest possible string of digits, that is, a pattern such as "12+67" matches "1234567", but does not match "1236767".	

Global Title Pattern configuration is viewed using the CNGPP MMI command. Global Title Patterns can be added to the config.txt file and then read into the system using the CNGPI command. Global Title Patterns are removed from the config.txt file and then removed from the system using the CNGPE MMI command.

5.10.7 SCCP_RSP - SCCP Remote Signaling Points

Synopsis

Each remote signaling point that the SCCP is able to communicate with must be assigned using an SCCP_RSP command. This includes the adjacent signaling point and all remote signaling points.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_RSP:[NC=NC0],SSRID=,SPC=[,OPTIONS=0][,PCMASK=0][,RIID=0][,LABEL=];
```

Example

```
SCCP_RSP:SSRID=1,SPC=1236;
```

Parameters

The SCCP_RSP command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2, or NC3.

- **SSRID**

A unique value in the range 0 to 2047 that is used to identify the SSR. 512 SSRIDs are allowed per Network Context. The same SSRID cannot be used in configuration of any other LSS, RSP or RSS.

- **SPC**

The point code of the remote signaling point, which may be either an STP or an SCP.

- **OPTIONS**

A 16-bit value, where each bit enables or disables additional features of the remote signaling point. The meaning for each bit is as defined for the options parameter defined in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.

- **PCMASK**

A 32-bit value that specifies the part of a destination point code that must match the <remote_spc> value in order for an SCCP transmit message to be sent down to this destination sub-system. Bits set to zero indicate that the corresponding bit position in the transmit message destination point code must match the bit position of the remote SPC. Bits set to 1 indicate bit positions in the message destination point code that do not need to match the remote SPC set for this RSP. This allows configuration of a default destination sub-system (for example, a gateway SCP).

- **RIID**

Routing Indicator ID.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

SCCP Remote Signaling Point configuration is viewed using the CNSSP MMI. After startup additional Remote Signaling Points can be added to the config.txt file and then read into the system using the CNSSI command. Remote Signaling Points are removed from the config.txt file and then removed from the system using the CNSSE MMI command.

5.10.8 SCCP_LSS - SCCP Local Sub-Systems

Synopsis

Each local SCCP sub-system is configured using an SCCP_LSS command, specifying the local sub-system number (as used by the SS7 protocol) and the module ID designated by the user to implement this sub-system.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_LSS:[NC=NC0],SSRID=,SSN=,LSSPROT=[,USER_ID=0x1d][,OPTIONS=0][,LABEL=];
```

Example

```
SCCP_LSS:[NC=NC0],SSRID=,SSN=0x7,LSSPROT=MAP,USER_ID=0x0d,OPTIONS=1;
```

Parameters

The SCCP_SSR command includes the following parameters when configuring SCCP local sub-systems:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.

- **SSRID**

A unique value in the range 0 to 2047 that is used to identify the SSR. 512 SSRIDs are allowed per Network Context. The same SSRID cannot be used in configuration of any other LSS, RSP or RSS.

- **SSN**

The local sub-system number as defined by the SCCP protocol.

- **USER_ID**

For SIU mode this is the module identifier of the user application on the host computer that implements the local sub-system. This must be in the range 0x0d, 0x1d, 0x2d to 0xfd, where 0xnd is defined as APPn_TASK_ID.

For SWS mode set to 0x45 for correct SWS operation.

- **OPTIONS**

A 16-bit value where each bit enables or disables additional features of the local sub-system. The meaning of each bit is as defined for the **options** parameter described in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.

- **LSSPROT**

For SIU mode set to SCCP, TCAP, MAP, IS41, INAP, DTS, DTS-MAP, DTS-INAP, or DTS-IS41 depending on the layer of the protocol stack that the user application interfaces with.

For SWS mode set to MAP.

For example, for SIU, to configure a local sub-system (SSN=6) for an application with module_id = 0x3d that implements an HLR by directly interfacing to MAP, the following command would be used:

SCCP_LSS 3 0x06 0x3d 0x0000 MAP

Additionally for example for SWS operation, to configure a local sub-system (SSN=8) for use in SWS mode the following command would be used:

SCCP_LSS 3 0x08 0x45 0x0000 MAP

Note: The MAP, IS41 and INAP modules currently support only a single user module each, therefore all MAP, IS41 or INAP local-sub-systems must use the same <module_id> value.

Note: Different local subsystems may specify different DTS variants; however, the DTS protocol and the non-DTS protocol cannot be specified simultaneously (e.g., MAP and DTS-MAP may not be specified at the same time).

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

SCCP Local Sub System configuration is viewed using the CNSSP MMI. The status of DTS SCCP Local hosts can read using the STDHP MMI command.

5.10.9 SCCP_RSS - SCCP Remote Sub-Systems

Synopsis

This command defines a remote sub-system known to the Signaling Server Signaling Server. Each entry contains the signaling point code and sub-system number. Multiple SCCP_SSR entries may be included in the file. The presence of an RSS command causes the SCCP to generate sub-system test (SST) messages for the sub-system.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_RSS:[NC=NC0],SSRID=,SPC=,SSN=[,OPTIONS=0][,LABEL=];
```

Example

```
SCCP_RSS:NC=NC1,SSRID=4,SPC=1234,SSN=0x67;
```

Parameters

The SCCP_RSS command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2, or NC3.

- **SSRID**

A unique value in the range 0 to 2047 that is used to identify the SSR. 512 SSRIDs are allowed per Network Context. The same SSRID cannot be used in configuration of any other LSS, RSP or RSS.

- **SPC**

The point code where the remote sub-system is implemented.

Note: For correct operation, <remote_spc> must always have its own SCCP_RSP entry in addition to any SCCP_RSS entries. There must also be an MTP_ROUTE defined for this signaling point.

- **SSN**

The remote sub-system number as defined by the SCCP protocol.

- **OPTIONS**

A 16-bit value where each bit enables or disables additional features of the remote sub-system. The meaning for each bit is as defined for the **options** parameter described in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.

- **LABEL**

A user configurable text string containing up to 32 characters used for identification purposes. The parameter is optional.

SCCP Remote Sub System configuration is viewed using the CNSSP MMI. After startup additional Remote Sub System Resources can be added to the config.txt file and then read into the system using the CNSSI command. Remote Sub System Resources are removed from the config.txt file and then removed from the system using the CNSSE MMI command.

5.10.10 SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration

Synopsis

This command defines an SCCP concerned resource that receives SCCP notifications if the state of a resource it is concerned about changes. A concerned sub-system resource, (CSSR), can refer to up to 32 sub-system resources, (SSR).

Notification is given in the form of an SCCP management indication. Multiple SCCP_CONC_SSR entries may be included in the file. See the *SCCP Programmer's Manual* for more information.

> ***Note:*** Attempting to mix the current command formats with the formats of older versions of commands within the same configuration file may give rise to restart errors indicating “inconsistent command format”.

Applicability

SIU, SWS, DSH

Syntax

```
SCCP_CONC_SSR:[NC=NC0],CSSRLID=,CSSRID=,SSRID=;
```

Example

```
SCCP_CONC_SSR:CSSRLID=1,CSSRID=4,SSRID=2;
```

Parameters

The SCCP_CONC_SRR command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.

- **CSSRLID**

A unique value in the range 0 to 8191 that is used to identify the concerned sub-system resource command.

- **CSSRID**

Refers to a concerned resource specified by either a SCCP_LSS or SCCP_RSP command. The CSSRID identifies the concerned resource that receives SCCP notifications if the state of the controlled resource identified by the SSRID is changed.

- **SSRID**

Refers to a controlled resource specified by either a SCCP_LSS or SCCP_RSP command:

— If the CSSRID is referring to an LSS, the SSRID used in the same command may refer to either an RSS or an RSP resource.

— If the CSSRID is referring to an RSP, the SSRID used in the same command can only refer to an LSS resource.

Note: The CSSRID and SSRID parameters can only refer to SSR's previously configured using either a SCCP_LSS or SCCP_RSP command.

SCCP Concerned Sub System Resource configuration is viewed using the CNCSP MMI. After startup additional Concerned Sub System Resource configuration can be added to the config.txt file and then read into the system using the CNCSI command. Concerned Sub System Resources configuration can be removed from the config.txt file and then removed from the system using the CNCSE MMI command.

5.11 DTS Configuration Commands

5.12 The DTS configuration commands include the following:

- DTS CONFIG - Distributed Transaction Server Configuration
- DTS_ROUTE - Configuration DTS Route Initiate

5.12.1 DTS_CONFIG - Distributed Transaction Server Configuration

Synopsis

The DTS_CONFIG command is an optional command that defines the global configuration parameters for DTS. Its principal function is to allow users to specify more than 16 TCAP hosts. Applications that operate on more than 16 TCAP hosts require a slightly different TCAP configuration from those that operate with 16 or less, as the transaction id (tid) requires more of its bits to be used to identify the TCAP instance. This command allows users to configure DTS on the SIU so that DTS matches TCAP configuration on the host.

Applicability

SIU

Syntax

```
DTS_CONFIG <NUM_HOSTS> <OPTIONS>
```

Example

```
DTS_CONFIG 20 0x0001
```

Parameters

The DTS_CONFIG command includes the following parameters:

- **NUM_HOSTS**

The number of SIU hosts which will receive traffic from DTS. When the DTS_CONFIG command is not used, this parameter default to 16 hosts.

> ***Note:*** For routing by BillingID the number of the hosts should be set accurately to optimize the routing algorithm.

- **OPTIONS**

Set bit 0 to enable routing by BillingID (DTS_OPT_RT_ON_BILLINGID).

5.12.2 DTS_ROUTE - Configuration DTS Route Initiate

Synopsis

Command to configure a DTS Route.

Syntax

```
DTS_ROUTE:drid=,hostid=,[nc=,][ssn=,][clseq=,][options=,][label=];
```

Example

```
DTS_ROUTE:drid=1,hostid=1,nc=NC1,ssn=8;
DTS_ROUTE:drid=2,hostid=1,ssn=6,clseq=1,options=0x0001,label=User App 1;
```

Parameters

- **DRID**

A DTS routing request id to uniquely identify a particular DTS routing request. An integer in the range 0-4095.

- **NC**

SS7 Network Context. This parameter identifies the SS7 network in which the subsystem exists. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is omitted, a value of NC0 is assumed.

- **HOSTID**

Logical identifier to identify each link from the SIU to a Client Host. Host 0 is on Link 0 and so on. An integer in the range 0-127.

- **SSN**

Subsystem Number to route to. If unspecified (or zero) then this will be the default subsystem used when no match occurs with any other SSN defined. An integer in the range 0-255.

- **CLSEQ**

The client sequence number within a client selection group (all routing requests that have the same NC+SSN combination). MUST be unique within the client selection group. An integer in the range 0-127.

- **OPTIONS**

Routing options for the DTS routing request - this is used to select 'strict routing' or 'preferred order' (see *DTS User Guide*).

- **LABEL**

A text string up to 32 character long.

5.13 TCAP Configuration Commands

The TCAP configuration commands include:

- TCAP_CONFIG - TCAP Configuration
- TCAP_NC_CONFIG - TCAP Network Context Configuration
- TCAP_CFG_DGRP - TCAP Dialog Group Configuration
- TCAP_TIMER - TCAP Timer Configuration

5.13.1 TCAP_CONFIG - TCAP Configuration

Synopsis

The TCAP_CONFIG command activates the TCAP protocol layer on the Signaling Server and provides the TCAP operating parameters. This command should only be used when an SCCP_CONFIG command is present.

Note: Network Context-specific configuration may be done using the TCAP_NC_CONFIG command.

Applicability

SIU, SWS, DSH

Syntax

```
TCAP_CONFIG <BASE_ODLG> <NUM_ODLG> <BASE_IDLG> <NUM_IDLG> <OPTIONS> <DLG_HUNT> <ADDR_FMT>
```

Examples

```
TCAP_CONFIG 0x0000 8192 0x8000 8192 0x0000 0 0
```

Parameters

The TCAP_CONFIG command includes the following parameters:

- **BASE_ODLG**

The dialogue_id for the first outgoing dialog.

- **NUM_ODLG**

The number of outgoing dialogs to support. The valid range is 0 to 32767.

- **BASE_IDLG**

The dialogue_id for the first incoming dialog. The most significant bit (bit 15) of the dialog ID must be set to one for incoming dialogs.

- **NUM_IDLG**

The number of incoming dialogs to support. The valid range is 0 to 32767.

Note: If dialogue values are out of the permitted range TCAP will be configured with default values of 32767 nog_dialogues and 32767 nic_dialogues.

- **OPTIONS**

Specifies TCAP protocol options as defined for the TCAP Configuration Request message in the *TCAP Programmer's Manual*.

- **DLG_HUNT**

The hunt mode used in the case of multiple TCAP hosts to determine which TCAP group is selected whenever a new incoming dialog arrives. It should be set to 0, 1 or 2 for the following hunt modes:

— 0: Cyclic Selection. Each new incoming dialog is allocated to the next TCAP group.

— 1: Load Balanced Selection. Each new incoming dialog is allocated to the group with the least number of active incoming dialogs.

— 2: Sequential Selection. Each new incoming dialog is allocated to the group containing the first inactive incoming <dialogue_id>.

- **ADDR_FMT**

The format of messages used by TCAP. Possible values are:

— 0: The address format is determined by the setting of bit 1 of the **<options>** field.
- If bit 1 of the **<options>** field is set to indicate ANSI TCAP PDU formats, then ANSI format 24-bit point codes are selected.
- If bit 1 of the **<options>** field is not set, ITU-T TCAP PDU formats and 14-bit point codes are selected.

— 1: ITU-T format, 14-bit point codes

— 2: ITU-T format, 24-bit point codes

— 3: ANSI format, 14-bit point codes

— 4: ANSI format, 24-bit point codes

Note: 16-bit point codes are not supported.

5.13.2 TCAP_NC_CONFIG - TCAP Network Context Configuration

Synopsis

The TCAP_NC_CONFIG command specifies Network Context-specific configuration for TCAP and overrides configuration specified by the TCAP_CONFIG command. This command should only be used when a TCAP_CONFIG command is present.

Applicability

SIU, DSH

Syntax

```
TCAP_NC_CONFIG <NC> <OPTIONS> <ADDR_FMT>
```

Examples

```
TCAP_NC_CONFIG NC0 0x0000 0
```

Parameters

The TCAP_NC_CONFIG command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that TCAP is being configured for. Supported values are: NC1, NC2 or NC3.

- **OPTIONS**

Specifies TCAP protocol options as defined for the TCAP Configuration Request message in the *TCAP Programmer's Manual*.

- **ADDR_FMT**

The format of messages used by TCAP. Possible values are:

— 0: The address format is determined by the setting of bit 1 of the **<options>** field.
- If bit 1 of the **<options>** field is set to indicate ANSI TCAP PDU formats, then ANSI format 24-bit point codes are selected.
- If bit 1 of the **<options>** field is not set, ITU-T TCAP PDU formats and 14-bit point codes are selected.

— 1: ITU-T format, 14-bit point codes

— 2: ITU-T format, 24-bit point codes

— 3: ANSI format, 14-bit point codes

— 4: ANSI format, 24-bit point codes

Note: 16-bit point codes are not supported.

5.13.3 TCAP_CFG_DGRP - TCAP Dialog Group Configuration

Synopsis

The TCAP_CFG_DGRP command allows you to configure TCAP dialog groups, each group handling a sub-set of the total available dialogs. This allows each group to reside on a separate host computer that in turn allows the application using TCAP to be distributed over several machines. If the TCAP_CFG_DGRP command is omitted, the complete range of dialog identifiers defined by the TCAP_CONFIG command is assigned to host_id 0.

Applicability

SIU, SWS, DSH

Syntax

```
TCAP_CFG_DGRP <DLGGID> <BASE_ODLG> <NUM_ODLG> <BASE_IDLG> <NUM_IDLG> <OPTIONS> <USER_HOST>
```

Examples

```
TCAP_CFG_DGRP 0 0x0000 1024 0x8000 1024 0 0
TCAP_CFG_DGRP 1 0x0400 1024 0x8400 1024 0 1
```

Parameters

The TCAP_CFG_DGRP command includes the following parameters:

- **DLGGID**

A logical identifier for this group, the valid range being 0 to 31.

- **BASE_ODLG**

The first outgoing dialog ID assigned to this dialog group.

- **NUM_ODLG**

The number of outgoing dialogs assigned to this group, hence outgoing dialog IDs base_ogdlg_id to base_ogdlg_id + nog_dialogues-1 are assigned to this group.

- **BASE_IDLG**

The first incoming dialog ID assigned to this dialog identifier group.

- **NUM_IDLG**

The number of incoming dialogs assigned to this group, hence outgoing dialog IDs base_ogdlg_id to base_icdlg_id + nic_dialogues-1 are assigned to this group.

- **OPTIONS**

Should be set to zero.

- **USER_HOST**

Identifies the host computer to which the defined ranges of dialogs will be sent.

The number of dialogs must lie within the limit specified with the TCAP_CONFIG command.

5.13.4 TCAP_TIMER - TCAP Timer Configuration

Synopsis

The TCAP_TIMER command provides the ability to configure the TCAP protocol timers from the config.txt file. This command is currently only used to configure the TCAP idle dialog timeout.

Applicability

SIU, SWS, DSH

Syntax

```
TCAP_TIMER 0 TDLG_IDLE_TOUT <TVAL>
```

Example

```
TCAP_TIMER 0 TDLG_IDLE_TOUT 10
```

Parameters

The TCAP_TIMER command includes the following parameters:

- **RESERVED**

Reserved for future use. Should be set to 0.

- **TIMID**

A text identifier for the timer to be configured. It should be set to TDLG_IDLE_TOUT.

- **TVAL**

The timer value in seconds.

5.14 MAP Configuration Commands

The MAP configuration commands include:

- MAP_CONFIG - MAP Configuration
- MAP_NC_CONFIG - MAP Configuration

5.14.1 MAP_CONFIG - MAP Configuration

Synopsis

The MAP_CONFIG command defines the global configuration parameters for MAP when existing in a single network or for Network Context 0 (NC0) when existing in multiple Network Contexts. See Section 7.4, “Configuring Multiple Network Contexts” on page 368 for more information. This command should only be used if the MAP software has been licensed and configured on the Signaling Server and must appear on a separate command line in the config.txt file after the SCCP_LSS command that identifies MAP as the protocol module.

Applicability

SIU, SWS, DSH

Syntax

```
MAP_CONFIG <OPTIONS>
```

Example

```
MAP_CONFIG 2
```

Parameters

The MAP_CONFIG command includes the following parameter:

- **OPTIONS**

A 32-bit value containing run-time options for passing to the MAP module. Individual bit definitions are as specified for the options field in the MAP_MSG_CONFIG command as defined in the *MAP Programmer’s Manual*. Currently, this includes two bits as follows:

Bit	Mnemonic	Description
0	MAPF_V2_ERRORS	V3 dialogs use the V2 error format
1	MAPF_NO_PREARRANGED_END	Dialogs are closed immediately on reception of CLOSE_REQ

5.14.2 MAP_NC_CONFIG - MAP Configuration

Synopsis

The MAP_NC_CONFIG command defines the global configuration parameters for MAP existing in an additional SS7 Network Context to that identified by the MAP_CONFIG command. See Section 7.4, “Configuring Multiple Network Contexts” on page 368 for more information.

Applicability

SIU

Syntax

```
MAP_NC_CONFIG <NC> <OPTIONS>
```

Example

```
MAP_NC_CONFIG NC1 2
```

Parameters

The MAP_NC_CONFIG command includes the following parameter:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that MAP is being configured for. Supported values are: NC1, NC2 or NC3.

- **OPTIONS**

A 32-bit value containing run-time options for passing to the MAP module. Individual bit definitions are as specified for the options field in the MAP_MSG_CONFIG command as defined in the *MAP Programmer’s Manual*. Currently, this includes two bits as follows:

Bit	Mnemonic	Description
0	MAPF_V2_ERRORS	V3 dialogs use the V2 error format
1	MAPF_NO_PREARRANGED_END	Dialogs are closed immediately on reception of CLOSE_REQ

5.15 IS41 Configuration Commands

There are currently no supported IS41 configuration commands.

5.16 INAP Configuration Commands

The INAP configuration commands include:

- INAP_CONFIG - INAP Configuration
- INAP_NC_CONFIG - INAP Network Context Configuration
- INAP_AC - INAP Application Contexts
- INAP_FE - INAP Functional Entities

5.16.1 INAP_CONFIG - INAP Configuration

Synopsis

The INAP_ CONFIG command defines the global configuration parameters for INAP when existing in a single network or for Network Context 0 (NC0) when existing in multiple Network Contexts. See Section 7.4, “Configuring Multiple Network Contexts” on page 368 for more information. This command should only be used if the INAP software has been licensed and configured on the Signaling Server.

Applicability

SIU

Syntax

```
INAP_CONFIG <OPTIONS>
```

Example

```
INAP_CONFIG 0
```

Parameters

The INAP_CONFIG command includes the following parameter:

- **OPTIONS**

A 32-bit value that contains run time options for the operation of the INAP protocol. The bits are as defined for the **options** parameter described in the Configuration Request section of the *INAP Programmer's Manual*.

5.16.2 INAP_NC_CONFIG - INAP Network Context Configuration

Synopsis

The INAP_NC_CONFIG command defines the global configuration parameters for INAP existing in an additional SS7 Network Context to that identified by the INAP_CONFIG command.

Applicability

SIU

Syntax

```
INAP_NC_CONFIG <NC> <OPTIONS>
```

Example

```
INAP_NC_CONFIG 0
```

Parameters

The INAP_NC_CONFIG command includes the following parameter:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network that INAP is being configured for. Supported values are: NC1, NC2 or NC3.

- **OPTIONS**

A 32-bit value that contains run time options for the operation of the INAP protocol. The bits are as defined for the options parameter described in the Configuration Request section of the *INAP Programmer's Manual*.

5.16.3 INAP_FE - INAP Functional Entities

Synopsis

This command is used to configure the INAP functional entity records for operation. These allow the user application to refer to Functional Entities (FEs) in the network via a local reference rather than providing the full SCCP. You may subsequently use this reference in the "Destination FE" or "Originating FE" parameters of the INAP_OPEN_DLG primitive or "IN_dialogue_open" API function. This reference is used instead of the destination or origination address parameter.

Applicability

SIU

Syntax

```
INAP_FE <NC> <FE_REF> <OPTIONS> <SCCP_ADDR>
```

Example

```
INAP_FE 0x00000007 0x01 0x430100f0
INAP_FE NC1 0x00000008 0x01 0x430200f0
```

Parameters

The INAP_FE command includes the following parameters:

- **NC**

SS7 Network Context. This parameter uniquely identifies the SS7 network the FE is being configured for. Supported values are: NC0, NC1, NC2 or NC3. When not specified, a value of NC0 is assumed.

- **FE_REF**

Logical identifier for this Functional Entity (FE) in the range 0 to 127 (max 128), with a maximum of 32 identifiers per Network Context.

- **OPTIONS**

A 16-bit FE options value. Bit 0 set to 1 identifies a local FE. Other bits should be set to 0.

- **SCCP_ADDR**

The SCCP address of the local FE, in Q.713 format commencing with the address indicator, as a string of hex characters, up to 18 characters in length.

The Signaling Server supports up to 32 functional entities.

5.16.4 INAP_AC - INAP Application Context

Synopsis

This command is used to configure the INAP Application Context (AC) records for use. These control the application context negotiation that the module conducts during dialog establishment. All supported application contexts must be individually configured using this message.

The module only accepts incoming dialogs with configured Application Contexts. If a dialog request with an unconfigured context is received, a dialog abort message is returned to the requesting Functional Entity.

If no supported Application Contexts are configured, the application context negotiation is disabled. The module accepts all incoming dialogs.

Applicability

SIU

Syntax

```
INAP_AC <AC_REF> <AC>
```

Example

```
INAP_AC  0x00  0xa109060704000101010000
```

Parameters

The INAP_AC command includes the following parameters:

- **AC_REF**

A logical identifier for this application context.

- **AC**

Application context. Specified as hexadecimal characters, prefixed by “0x”. An application context may be up to 32 octets (character pairs) in length. The Signaling Server supports up to 32 application contexts.

6 Management Commands

The following is a summary of the command categories and the commands within those categories.

Help for these commands is also available on line using MMI by simply typing a '?' character followed by the return character at the MML command enter prompt.

6.1 Access Control Commands

“ACCUP - Access Current User Configuration”

“ACCUS - Account Control Current User Set”

“ACPOP - Account Control Policy Configuration”

“ACPOS - Account Control Policy Set”

“ACUAE - Account Control User Account End”

“ACUAI - Account Control User Account Initiate”

“ACUAP - Account Control User Account Configuration”

“ACUPC - Account Control User Profile Change”

“ACUPE - Account Control User Profile End”

“ACUPI - Account Control User Profile Initiate”

“ACUPP - Account Control User Profile Configuration”

“ALLIP - Active Alarm List”

6.1.1 ACCUP - Access Current User Configuration

This command displays information related to a specific user account. In the output, a PASSWORD (and the associated CONFIRM) value will be displayed "*********".

Syntax

ACCUP;

Web Management Location

System Administration > Access Control > Current User > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Example

ACCUP;

Output Format

```
User Password Configuration
USER       john
PASSWORD   ********
CONFIRM    ********
```

6.1.2 ACCUS - Account Control Current User Set

This command changes configuration data for the current user.

Syntax

ACCUS:PASSWORD=,CONFIRM=;

Web Management Location

System Administration > Access Control > Current User > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Prerequisites

The character strings for the password and confirm parameters must be identical.

Example

ACCUS:PASSWORD=Di@l0gic,CONFIRM=Di@l0gic;

6.1.3 ACPOP - Account Control Policy Configuration

This command displays the access policy for a server.

Syntax

ACPOP;

Web Management Location

System Administration > Access Control > System Policy > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

ACPOP;

Output Format

```
Account Control Policy Configuration
TELSER      ACTIVE
SSHSER      ACTIVE
FTPSER      ACTIVE
WMSER       ACTIVE
WSSER       ACTIVE
SESSIONS    STATIC_TAGS
MAXLIFE
STRONG      Y
RPFILTER    1
```

6.1.4 ACPOS - Account Control Policy Set

This command changes the access policy for a server.

Syntax

ACPOS:[TELSER=,][SSHSER=,][FTPSER=,][WMSER=,][WSSER=,][SESSIONS=,][MAXLIFE=,][STRONG=,];[RPFILTER=,]

Web Management Location

System Administration > Access Control > System Policy > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Policy Management Access

Example

ACPOS:MAXLIFE=30;

6.1.5 ACUAC - Account Control User Account Change

This command changes the configuration of a user account.

Syntax

ACUAC:USER=,[PASSWORD=, CONFIRM=,][ACCESS=,];

Web Management Location

System Administration > Access Control > User Accounts > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Administration Access

Prerequisites

When entered, the character strings for the password and confirm parameters must be identical.

Example

ACUAC:USER=admin,PASSWORD=Di@l0gic,CONFIRM=Di@l0gic;

6.1.6 ACUAE - Account Control User Account End

This command deletes a user account.

Syntax

ACUAE:USER=;

Web Management Location

System Administration > Access Control > User Accounts > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Administration Access

Example

ACUAE:USER=operator1;

6.1.7 ACUAI - Account Control User Account Initiate

This command adds a user account.

Syntax

ACUAI:USER=,PASSWORD=,CONFIRM=,ACCESS=,;

Web Management Location

System Administration > Access Control > User Accounts > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Administration Access

Prerequisites

The character strings for the password and confirm parameters must be identical.

Example

ACUAI:USER=operator1,PASSWORD=Di@l0gic,CONFIRM=Di@l0gic,ACCESS=operator;

6.1.8 ACUAP - Account Control User Account Configuration

This command displays information related to user accounts. In the output a PASSWORD (and the associated CONFIRM) value will be displayed as "********"

Syntax

ACUAP;

Web Management Location

System Administration > Access Control > User Accounts > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

ACUAP;

Output Format

```
User Account Configuration
USER                 PASSWORD CONFIRM  ACCESS
admin                ******** ******** policy
ftpuser              ******** ******** ftponly
john                 ******** ******** operator
```

6.1.9 ACUPC - Account Control User Profile Change

This command changes the configuration of a user profile.

Syntax

ACUPC:ACCESS=,[CLI=,][FTP=,][MWS=,][WSS=,][MGR=,][MGW=,][MGX=,][MGA=,][MGS=,][MGP=,][EXP=,];

Applicability

DSH

Web Management Location

System Administration > Access Control > User Profile > ConfigurationOperating Modes: SIU, SWS

Permissions: Policy Management Access

Example

ACUPC:ACCESS=admin,MGW=Y;

6.1.10 ACUPE - Account Control User Profile End

This command deletes a user profile.

Syntax

ACUPE:ACCESS=;

Applicability

DSH

Web Management Location

System Administration > Access Control > User Profile > ConfigurationApplicability

Operating Modes: SIU, SWS

Permissions: Policy Management Access

Example

ACUPE:ACCESS=admin;

6.1.11 ACUPI - Account Control User Profile Initiate

This command adds a user profile.

Syntax

ACUPI:ACCESS=,[CLI=,][FTP=,][MWS=,][WSS=,][MGR=,][MGW=,][MGX=,][MGA=,][[MGS=,][[MGP=,][EXP=,];

Applicability

DSH

Web Management Location

System Administration > Access Control > User Profile > ConfigurationApplicability

Operating Modes: SIU, SWS

Permissions: Policy Management Access

Example

ACUPI:ACCESS=admin,CLI=Y,FTP=Y,MWS=Y,WSS=Y,MGR=Y,MGW=Y,MGX=Y,MGA=Y,MEXP=Y;

6.1.12 ACUPP - Account Control User Profile Configuration

This command displays information related to user profiles.

When specified without a parameter or the page parameter the output provided is a table of privileges for all access policies. When specified with the ACCESS parameter (command line only) the output provides a textual description of each privilege associated with the access policy.

Syntax

ACUPP; ACUPP:[ACCESS=]; ACUPP:[PAGE=];

Applicability

DSH

Web Management Location

System Administration > Access Control > User Profile > ConfigurationApplicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

ACUPP; ACUPP:PAGE=2; ACUPP:ACCESS=policy;

Output Format

```
Access User Profile Configuration (Page 1 of 2)
ACCESS          CLI FTP MWS WSS EXP
policy          Y   Y   Y   N   Y
admin           Y   Y   Y   N   Y
operator        Y   Y   Y   N   Y
user            Y   N   Y   N   Y
ftponly         N   Y   N   N   N
wssonly         N   N   N   Y   N

Access User Profile Configuration (Page 2 of 2)
ACCESS          MGR MGW MGX MGS MGA MGP
policy          Y   Y   Y   Y   Y   Y
admin           Y   Y   Y   Y   Y   N
operator        Y   Y   Y   N   N   N
user            Y   N   N   N   N   N
ftponly         N   N   N   N   N   N
wssonly         N   N   N   N   N   N

Access User Profile Configuration
ACCESS   policy
CLI      Y              MML command line interface enabled
FTP      Y              FTP login read/write enabled
WMS      Y              Management web server enabled
WSS      N              Web Services API disabled
EXP      N              Password expiry disabled
MGR      Y              Read configuration status and measurements
MGW      Y              Change/Add/Delete configuration
MGX      Y              Maintenance actions (block/unblock/reset)
MGS      Y              Security management enabled
MGA      Y              Administrative access to add/remove users
MGP      Y              Policy access to set system policy
```

6.2 Alarm Commands

“ALLIP - Active Alarm List”

“ALLOP - Alarm Log”

“ALTEE - Alarm Test End”

“ALTEI - Alarm Test Initiate”

6.2.1 ALCDP - Alarm Codes

This command displays the list of alarm codes and the attributes associated with each code.

The attributes include the title, severity of the alarm (when active), type of alarm (communicationsAlarm (2), qualityOfServiceAlarm (3), processingErrorAlarm (4), equipmentAlarm (5) or environmentalAlarm (6)) and the probable cause of the alarm based on the principles of ITU Recommendations M.3100, X.733, and X.736 and GSM 12.10 (ETS 300 618).

Syntax

ALCDP;

Web Management Location

System Administration > Diagnostics > Alarm Code > Configuration

Applicability

Operating Modes: ALL, DSH

Permissions: Configuration Read Access

Example

ALCDP;

Output Format

Alarm Code Configuration

CODE	TITLE	SEVERITY	TYPE	CAUSE
1	PCM loss	MAJ	2	8
2	Sync loss	MAJ	2	6
4	AIS	MAJ	2	1
5	Remote Alarm	MAJ	2	571
6	BER5	MAJ	2	3
7	BER3	MAJ	2	12
8	PSU fail	CRT	5	522
9	SS7 link fail	MAJ	2	573
10	SS7 linkset lost	MAJ	2	573
12	SS7 link cong	MNR	3	308
13	Fan fail	CRT	6	107
14	Fan warning	MAJ	6	107
16	Temperature	CRT	6	123
17	Host link fail	CRT	2	566
18	Partner link fail	CRT	2	566
19	Parse errors	CRT	4	307
20	Config fail	CRT	4	307
22	System overload	MAJ	3	564
24	Evaluation mode	CRT	4	307
25	CPU temperature	MAJ	5	59
28	Board fail	CRT	5	68
30	CPU warning	MAJ	5	59
31	Voltage warning	MAJ	5	522
32	Memory warning	MAJ	4	152
34	Sigtran link fail	MAJ	2	566
38	Traffic congested	MNR	3	343
39	Traffic enforce	MAJ	3	343
41	Restart required	CRT	4	537
42	System restart	CRT	4	158
45	NTP sync fail	CRT	2	306
52	Drive unavail	MAJ	5	508
67	CMOS battery low	WRN	6	105
69	Insufficient hosts	CRT	2	306
70	SDP congestion	CRT	3	343
71	File sys warning	WRN	5	508
72	DB unavail	MAJ	2	17
73	CRT test alarm	CRT	2	570

```
74    MAJ test alarm      MAJ       2     570
75    MNR test alarm      MNR       2     570
78    SCTP path fail      MNR       2     574

EXECUTED
```

6.2.2 ALLIP - Active Alarm List

Command to display the list of any active alarms.

In the event that “Parse Errors” are listed as an active alarm, further information on the cause of the error can be obtained using page 2 of the command.

Syntax

ALLIP;

Web Management Location

System Administration > Diagnostics > Alarms > Status

Operations > Alarms

Footer > Alarms

Applicability

Operating Modes: ALL, DSH

Permissions: Configuration Read Access

Example

ALLIP;

Output Format

```
Active Alarm List
  Active Alarm List (Page 1 of 2)
  SEQUENCE   CODE STATE SEVERITY ID    DIAG1      DIAG2      OCCURRED            TITLE               TYPE CAUSE
  43         34   ACT   MAJ      8     0          0          2014-04-11 09:58:44 Sigtran link fail   2    566
  42         34   ACT   MAJ      7     0          0          2014-04-11 09:58:44 Sigtran link fail   2    566
  41         34   ACT   MAJ      6     0          0          2014-04-11 09:58:44 Sigtran link fail   2    566
  40         34   ACT   MAJ      5     0          0          2014-04-11 09:58:44 Sigtran link fail   2    566
  39         10   ACT   MAJ      1     0          0          2014-04-11 09:58:44 SS7 linkset lost    2    573
  38         19   ACT   CRT      0     0          0          2014-04-11 09:58:38 Parse errors        4    307
  37         35   ACT   MAJ      8     0          0          2014-04-11 09:58:38 Sigtran Assoc fail  2    566
  36         35   ACT   MAJ      7     0          0          2014-04-11 09:58:38 Sigtran Assoc fail  2    566
  35         35   ACT   MAJ      6     0          0          2014-04-11 09:58:38 Sigtran Assoc fail  2    566
  34         35   ACT   MAJ      5     0          0          2014-04-11 09:58:38 Sigtran Assoc fail  2    566

  Active Alarm List (Page 2 of 2)
  ID    CONFIGURATION_ERROR
  86    Parse error: STN_LINK unknown parameter (syntax error)
  144   Parse error: MTP_LINK bad value (BLINK)
  151   Parse error: MTP_ROUTE data component exists (C7RT)
```

6.2.3 ALLOP - Alarm Log

Command to display a log of recent alarm events and, where applicable, the time that the alarm cleared. This command displays up to 1,000 alarms.

Syntax

ALLOP;

Web Management Location

System Administration > Diagnostics > Alarms > Log

Applicability

Operating Modes: ALL, DSH

Permissions: Configuration Read Access

Example

ALLOP;

Output Format

```
Alarm Log
  SEQUENCE   CODE STATE SEVERITY ID    DIAG1      DIAG2      OCCURRED            CLEARED             TITLE              TYPE CAUSE
  5          19   ACT   CRT      0     0          0          2014-04-15 12:24:04                     Parse errors       4    307
  4          18   ACT   CRT      0     0          0          2014-04-15 12:24:04                     SIU link failed    2    566
  3          17   CLR   CLR      0     0          0          2014-04-15 12:24:04 2014-04-15 12:24:07 Host link failed   2    566
  2          69   CLR   CLR      0     0          0          2014-04-15 12:24:04 2014-04-15 12:24:07 Insufficient hosts 2    306
  1          42   ACT   CRT      0     0          0          2014-04-15 12:24:03

System restarting  4    158
```

6.2.4 ALTEE - Alarm Test End

Clears a test alarm.

Syntax

ALTEE:{[CLA=5]|[CLA=4]|[CLA=3]};

Web Management Location

System Administration > Diagnostics > Alarm Test > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Example

ALTEE:CLA=3;

6.2.5 ALTEI - Alarm Test Initiate

The command generates an active test alarm of the specified class, which is entered in the alarm log. Alarm tests can be used to validate the operation of hardware such as LEDS on the front panel of the server.

Syntax

ALTEI:{[CLA=5]|[CLA=4]|[CLA=3]};

Web Management Location

System Administration > Diagnostics > Alarm Test > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Example

ALTEI:CLA=3;

6.3 Configuration Commands

"CNACE - ATM Cell Stream End"

"CNACI - ATM Cell Stream Initiate"

"CNACP - ATM Cell Stream Configuration"

"CNBOP - Board Configuration"

"CNBOS - Board Set"

"CNCGE - Circuit Group End"

"CNCGI - Circuit Group Initiate"

"CNCGP - Circuit Group Configuration"

"CNCRE - SS7 Route End"

"CNCRI - SS7 Route Initiate"

"CNCRP - SS7 Route Configuration"

"CNCSE - SCCP Concerned Subsystem Resource End"

"CNCSI - SCCP Concerned Subsystem Resource Initiate"

"CNCSP - SCCP Concerned Subsystem Resource Configuration"

"CNDRE - DTS Host Route End"

"CNDRI - DTS Host Route Initiate"

"CNDRP - DTS Host Routing Resource Print"

"CNDUP - Dual Operation Configuration"

"CNGAE - SCCP GTT Address End"

"CNGAI - SCCP GTT Address Initiate"

"CNGAP - SCCP GTT Address Configuration"

"CNGLE - SIGTRAN Gateway List End"

“CNGLI - SIGTRAN Gateway List Initiate”

“CNGLP - SIGTRAN Remote Signaling Gateway List Configuration”

“CNGPE - SCCP GTT Pattern End”

“CNGPI - SCCP GTT Pattern Initiate”

“CNGPP - SCCP GTT Pattern Configuration”

“CNGTE - SCCP GTT Translation End”

“CNGTI - SCCP GTT Translation Initiate”

“CNGTP - SCCP GTT Translation Configuration”

“CNHSP - Host Configuration”

“CNLAE - SIGTRAN Local Application Server End”

“CNLAI - SIGTRAN Local Application Server Initiate”

“CNLAP - SIGTRAN Local Application Server Configuration”

“CNLCP - Software License Capability Configuration”

“CNLDE - SCCP Loadshare DPC Configuration End”

“CNLDI - SCCP Loadshare DPC Configuration”

“CNLDP - SCCP Loadshare DPC Configuration”

“CNLSE - SS7 Link Set End”

“CNLSI - SS7 Link Set Initiate”

“CNLSP - SS7 Link Set Configuration”

“CNLTE - SCCP Loadshare Table Configuration End”

“CNLTI - SCCP Loadshare Table Configuration”

“CNLTP - SCCP Loadshare Table Configuration”

“CNMLE - SS7 Monitor Link End”

“CNMLI - SS7 Monitor Link Initiate”

“CNMLP - SS7 Monitor link Configuration”

“CNMNI / CNMNE - Multi-Node Configuration”

“CNMNP - Multi-Node Configuration Print”

“CNOBP - SNMP Trap Configuration”

“CNOBS - Configuration SNMP Traps Set”

“CNPCE - PCM End”

“CNPCI - PCM Initiate”

“CNPCP - PCM Configuration”

“CNRAE - SIGTRAN Remote Application Server End”

“CNRAI - SIGTRAN Remote Application Server Initiate”

“CNRAP - SIGTRAN Remote Application Server Configuration”

“CNRDI - Configuration Restore Default Initiate”

“CNRLE - SIGTRAN Remote Application Server List End”

“CNRLI - SIGTRAN Remote Application Server List Initiate”

“CNRLP - SIGTRAN Remote Application Server List Configuration”

“CNSBE - SIGTRAN Local Bind End”

“CNSBI - SIGTRAN Local Bind Initiate”

“CNSBP - SIGTRAN Local Bind Configuration”

“CNSLE - SS7 Link End”

“CNSLI - SS7 Link Initiate”

“CNSLP - SS7 Link Configuration”

“CNSMC - Configuration SNMP Manager Change”

“CNSME - Configuration SNMP Manager End”

“CNSMI - Configuration SNMP Manager Initiate”

“CNSMP - SNMP Manager Configuration”

“CNSNP - SNMP Configuration”

“CNSNS - Configuration SNMP Set”

“CNSRE - SIGTRAN Route End”

“CNSRI - SIGTRAN Route Initiate”

“CNSRP - SIGTRAN Route Configuration”

“CNSSE - SCCP Subsystem Resource End”

“CNSSI - SCCP Subsystem Resource Initiate”

“CNSSP - SCCP Subsystem Resource Configuration”

“CNSTE - SIGTRAN Link End”

“CNSTI - SIGTRAN Link Initiate”

“CNSTP - SIGTRAN Link Configuration”

“CNSWP - System Software Configuration”

“CNSYP - System Configuration”

“CNSYS - Configuration System Set”

“CNTDP - Time and Date Configuration”

“CNTDS - Configuration Time and Day Set”

“CNTMP - Trace Masks Configuration”

“CNTMS - Configuration Trace Mask Set”

“CNTPE - Configuration Network Time Protocol Server End”

“CNTPI - Configuration Network Time Protocol Server Initiate”

“CNTPP - NTP Server Configuration”

“CNURC - Configuration Update Resources Change”

“CNURE - Configuration Update Resources End”

“CNURI - Configuration Update Resources Initiate”

“CNUSC - Configuration SNMP User Change”

“CNUSE - Configuration SNMP User End”

“CNUSI - Configuration SNMP User Initiate”

“CNUSP - SNMP User Configuration”

6.3.1 CNACE - ATM Cell Stream End

This command removes an ATM Cell Stream.

Note: Cell Streams are dynamically removed by first deleting the cell stream from the config.txt file and then executing this command to unload the cell stream from the system.

Syntax

CNACE:CELLSTR=;

Web Management Location

System Administration > Boards > Cell Streams > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The ATM Cell Stream has been initiated.

The ATM Cell Stream is not present in the config.txt file.

The ATM Cell Stream is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

There are no startup parse or configuration errors present in the alarm log. The ATM Cell Stream is present in the config.txt file.

Example

CNACE:CELLSTR=1;

6.3.2 CNACI - ATM Cell Stream Initiate

This command adds a new ATM Cell Stream.

Note: ATM Cell Streams are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNACI:CELLSTR=;

Web Management Location

System Administration > Boards > Cell Streams > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The ATM Cell Stream ID has not been initiated.

The ATM Cell Stream is present in the config.txt file.

There are no startup parse or configuration errors present.

The ATM Cell Stream is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNACI:CELLSTR=1;

6.3.3 CNACP - ATM Cell Stream Configuration

This command displays the all configured ATM Cell Streams.

Syntax

CNACP;

Web Management Location

System Administration > Boards > Cell Streams > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNACP;

Output Format

```
ATM Cell Stream Configuration
CELLSTR BPOS L2ID PORTID     OPTIONS IMALEN DEFVPI DEFVCI
  1          0 1          1  0x0000 0      12     10
```

Note: See either the individual parameter definitions or the config.txt command "ATM_CELL_STREAM" for a full description of the parameters used in the output format.

6.3.4 CNBOP - Board Configuration

This command displays the configuration of all Signaling boards

Note: The board serial number does not need to be set or changed as it is determined automatically. If a board is added or replaced then the board type should be set (or unset and reset when replacing) and the system restarted after which it will extract the new serial number of the board.

Parameters associated the SS7_BOARD command in config.txt will only be displayed if a SS7_BOARD command is present for the board in config.txt.

Syntax

CNBOP;

Web Management Location

System Administration > Boards > Boards > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNBOP;

Output Format

```
Board Configuration
BPOS          BRDTYPE     OPTIONS
0             SS7MD       Ox00000001
1             SS7MD       Ox00000001
```

Note: See either the individual parameter definitions or the config.txt command "SS7_BOARD" for a full description of the parameters used in the output format.

6.3.5 CNBOS - Board Set

This command specifies the boards a user requires in a system.

Note: The board serial number does not need to be set or changed as it is determined automatically. If a board is added or replaced then the board type should be set (or unset and reset when replacing) and the system restarted after which it will extract the new serial number of the board.

Syntax

CNBOS:BPOS=,BRDTYPE=;

Web Management Location

System Administration > Boards > Boards > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The board type must match that of the fitted board in the specified position.

Example

CNBOS:BPOS=1,BRDTYPE=SS7MD;

6.3.6 CNCGE - Circuit Group End

This command removes a Circuit Group.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file and then executing this command to unload the group from the system.

Syntax

CNCGE:GID=;

Web Management Location

System Administration > Call > Circuit Groups > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The Circuit Group ID has been initiated.

The Circuit Group has been deactivated.

The Circuit Group is not used in any other configuration.

The Circuit Group is not present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The Circuit Group is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNCGE:GID=1;

6.3.7 CNCGI - Circuit Group Initiate

This command adds a new Circuit Group.

Note: Circuit Groups are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNCGI:GID=;

Web Management Location

System Administration > Call > Circuit Groups > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The Circuit Group ID has not been initiated.

The Circuit Group is present in the config.txt file.

There are no startup parse or configuration errors present.

The Circuit Group is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNCGI:GID=1;

6.3.8 CNCGP - Circuit Group Configuration

This command displays circuit group configuration data.

Syntax

CNCGP:[GID=][,PAGE=];

Web Management Location

System Administration > Call > Circuit Groups > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

CNCGP; CNCGP:PAGE=2; CNCGP:GID=0; CNCGP:GID=0,PAGE=2;

Output Format

```
Circuit Group Configuration (Page 1 of 2)
  GGID  NC  OPC      DPC      BCIC       BCID  CIC_MASK    VARIANT  OPTIONS    OPTIONS2   LABEL
  0     NC0 1        2        0          1     0xffffffff  ITU_2000 0x0000001c 0x00000000
  1     NC0 1        2        32         33    0xffffffff  ITU_2000 0x0000001c 0x00000000
  2     NC0 1        3        64         65    0xffffffff  ITU_2000 0x0000001c 0x00000000
  3     NC0 1        3        96         97    0xffffffff  ITU_2000 0x0000001c 0x00000000

Circuit Group Configuration (Page 2 of 2)
  GID  SSF USER_HOST USER_ID  MNGT_HOST MNGT_ID  MAINT_HOST MAINT_ID LABEL
  0    0x8 0         0x1d     0         0x1d     0          0x1d
  1    0x8 0         0x1d     0         0x1d     0          0x1d
  2    0x8 0         0x1d     0         0x1d     0          0x1d
  3    0x8 0         0x1d     0         0x1d     0          0x1d
```

See either the individual parameter definitions or the config.txt command "ISUP_CFG_CCTGRP" for a full description of the parameters used in the output format.

6.3.9 CNCRE - SS7 Route End

This command removes an MTP route.

Note: MTP routes are dynamically removed by first deleting the route from the config.txt file and then executing this command to unload the route from the system.

Syntax

CNCRE:C7RT=;

Web Management Location

System Administration > SS7 > SS7 Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The MTP Route ID has been initiated.

The MTP Route is not present in the config.txt file.

The MTP Route is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SS7 Route End is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNCRE:C7RT=1;

6.3.10 CNCRI - SS7 Route Initiate

This command adds a new MTP route.

Note: MTP routes are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Configuring a MTP route to an adjacent Signaling End Point (SEP) requires any/all previously configured MTP links that will be associated with the route to be taken out of service (deactivated) and then brought back into service (activated) to allow the route to come fully into service. New MTP routes that reach a destination via an STP do not require this additional step as they will come into service on the completion of the Signaling Route Set Test mechanism.

Syntax

CNCRI:C7RT=;

Web Management Location

System Administration > SS7 > SS7 Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The MTP Route ID has not been initiated.

The MTP Route is present in the config.txt file.

There are no startup parse or configuration errors present.

The SS7 Route Initiate is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNCRI:C7RT=1;

6.3.11 CNCRP - SS7 Route Configuration

This command displays MTP route configuration data,

Syntax

CNCRP:[C7RT=];

Web Management Location

System Administration > SS7 > SS7 Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNCRP; CNCRP:C7RT=0;

Output Format

```
SS7 Route Configuration
C7RT  NC      DPC         LS1     LS2         UPMASK    OPTIONS LABEL
0     NC0     1           0       0           0x00008   0x00000
1     NC0     2           0       0           0x00008   0x00000
2     NC1     3           0       0           0x00008   0x00000
```

See either the individual parameter definitions or the config.txt command "MTP_ROUTE" for a full description of the parameters used in the output format.

6.3.12 CNCSE - SCCP Concerned Subsystem Resource End

This command removes a Concerned Sub-System Resource.

Note: Concerned Sub-System Resources are dynamically removed by first deleting the Resource from the config.txt file and then executing this command to unload the Resource from the system.

Syntax

CNCSE:CSSRLID=;

Web Management Location

System Administration > Transaction > SCCP CSSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The Concerned Sub-System List ID has been initiated.

The Concerned Sub-System List ID is not present in the config.txt file.

The Concerned Sub-System is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The Concerned Sub-System Resource is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNCSE:CSSRLID=1;

6.3.13 CNCSI - SCCP Concerned Subsystem Resource Initiate

This command adds a new Concerned Sub-System Resource.

Note: Concerned Sub-System Resources are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNCSI:CSSRLID=;

Web Management Location

System Administration > Transaction > SCCP CSSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The Concerned Sub-System List ID has not been initiated.

The Concerned Sub-System List ID is present in the config.txt file.

There are no startup parse or configuration errors present.

The Concerned Sub-System Resource is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNCSI:CSSRLID=1;

6.3.14 CNCSP - SCCP Concerned Subsystem Resource Configuration

This command displays Concerned Sub-system configuration data.

Syntax

CNCSP:[CSSRLID=],[CSSR=],[NC=];

Web Management Location

System Administration > Transaction > SCCP CSSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNCSP; CNCSP:CSSR=LSS; CNCSP:NC=0;

Output Format

```
SCCP Concerned Subsystem Resource Configuration
CSSRLID  NC      CSSRID SSRID CSSR CSPC     CSSN SSR SPC      SSN
0        NC1     1      11    LSS           13   RSP 3
1        NC1     2      23    LSS           13   RSS 3        8
2        NC2     4      34    LSS           253  RSP 4
3        NC2     8      35    LSS           253  RSS 4        8
4        NC0     9      36    LSS           253  RSP 2
5        NC0     10     37    LSS           253  RSS 2        8
```

See either the individual parameter definitions or the config.txt command "SCCP_CONC_SSR" for a full description of the parameters used in the output format.

6.3.15 CNDRE - DTS Host Route End

This command removes an DTS Host Route.

Note: DTS Routes are dynamically removed by first deleting the DTS Route from the config.txt file and then executing this command to unload the DTS Route from the system.

Syntax

CNDRE:DRID=;

Web Management Location

System Administration > Transaction > DTS Route Requests > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The DTS Route has been initiated.
The DTS Route is not present in the config.txt file.
The DTS Route is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The DTS Host Route is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNDRE:DRID=1;

6.3.16 CNDRI - DTS Host Route Initiate

This command adds a new DTS Host Route. DTS Routes are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNDRI:DRID=;

Web Management Location

System Administration > Transaction > DTS Route Requests > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The DTS Route has not been initiated.
The DTS Route is present in the config.txt file.
There are no startup parse or configuration errors present.
The DTS Host Route is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

CNDRI:DRID=1;

6.3.17 CNDRP - DTS Host Routing Resource Print

This command is used to display any DTS host routing that was configured using the DTS_ROUTE command in config.txt. The CNDRP command is defined as follows:

Synopsis

This command displays DTS Host Routing configuration data.

Syntax

CNDRP:[DRID=,][NC=,][HOSTID=,];

Web Management Location

System Administration > Transaction > DTS Route Requests > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

CNDRP;
CNDRP:DRID=1;

Output Format

```
DTS Host Routing Configuration
DRID NC   HOSTID SSN CLSEQ OPTIONS LABEL
0    NC0  0      0    0    0x0000
1    NC1  1      8    0    0x0000
2    NC0  1      6    0    0x0001  User App 1
```

6.3.18 CNDUP - Dual Operation Configuration

This command displays Dual Server operation configuration.

Note: See the individual parameter definitions of the config.txt command SIU_DUAL defined in the user manual for a full description of the parameters supported.

Syntax

CNDUP;

Web Management Location

System Administration > Server Management > Dual Operation > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNDUP;

Output Format

```
Dual Operation Configuration
MODE                MODEA
REMOTE_IPADDR       192.168.0.1
```

See either the individual parameter definitions or the config.txt command "SIU_DUAL" for a full description of the parameters used in the output format.

6.3.19 CNGAE - SCCP GTT Address End

This command removes an SCCP GTT Address.

Note: SCCP GTT Addresses are dynamically removed by first deleting the Gateway List from the config.txt file and then executing this command to unload the Gateway List from the system.

Syntax

CNGAE:GTAID=;

Web Management Location

Administration > Transaction > GTT Addresses > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Address ID has been initiated.

The SCCP GTT Address is not present in the config.txt file.

The SCCP GTT Address is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SCCP GTT Address is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNGAE:GTAID=1;

6.3.20 CNGAI - SCCP GTT Address Initiate

This command adds a new SCCP GTT Address.

Note: SCCP GTT Addresses are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNGAI:GTAID=;

Web Management Location

System Administration > Transaction > GTT Addresses > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Address ID has not been initiated.

The SCCP GTT Address is present in the config.txt file.

There are no startup parse or configuration errors present.

The SCCP GTT Address is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNGAI:GTAID=1;

6.3.21 CNGAP - SCCP GTT Address Configuration

This command shows GTT Addresses defined on the system.

Syntax

CNGAP:[NC=,][GTAID=,];

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNGAP;

Output Format

```
SCCP  GTT Address Configuration
GTAID  NC        AI      SPC      SSN     GT                      GTAI_REPLACEMENT
4      NC0       0x11    4369      0      0x001104                333/---/4
5      NC0       0x11    17476     0      0x001104                55/
1023   NC1       0x11    21845     0      0x001104                00/
```

See either the individual parameter definitions or the config.txt command "SCCP_GTT_ADDRESS" for a full description of the parameters used in the output format.

6.3.22 CNGLE - SIGTRAN Gateway List End

This command removes an SIGTRAN Gateway List.

Note: SIGTRAN Gateway Lists are dynamically removed by first deleting the Gateway List from the config.txt file and then executing this command to unload the Gateway List from the system.

Syntax

CNGLE:GLID=;

Web Management Location

System Administration > SIGTRAN > Remote Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN Gateway List ID has been initiated.

The SIGTRAN Gateway List is not present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN Gateway List is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNGLE:GLID=1;

6.3.23 CNGLI - SIGTRAN Gateway List Initiate

This command adds a new SIGTRAN Gateway List.

Note: SIGTRAN Gateway Lists are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNGLI:SNRT=;

Web Management Location

System Administration > SIGTRAN > Remote Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN Gateway List ID has not been initiated.

The SIGTRAN Gateway List is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN Gateway List is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNGLI:SNRT=1;

6.3.24 CNGLP - SIGTRAN Remote Signaling Gateway List Configuration

This command displays the configuration of relationships between Signaling Gateways and SIGTRAN Routes on the system.

Syntax

CNGLP:[RSG=],;

Web Management Location

System Administration > SIGTRAN > Remote Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNGLP; CNGLP:RSG=3;

Output Format

```
SIGTRAN Remote Signaling Gateway List Configuration
GLID SNRT RSG OPTIONS
1    1    1   0x0001
2    1    2   0x0001
3    2    2   0x0001
4    3    1   0x0001
```

See either the individual parameter definitions or the config.txt command "STN_RSGLIST" for a full description of the parameters used in the output format.

6.3.25 CNGPE - SCCP GTT Pattern End

This command removes an SCCP GTT Pattern.

Note: SCCP GTT Patterns are dynamically removed by first deleting the Gateway List from the config.txt file and then executing this command to unload the Gateway List from the system.

Syntax

CNGPE:GTPID=;

Web Management Location

System Administration > Transaction > GTT Patterns > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Pattern ID has been initiated.

The SCCP GTT Pattern is not present in the config.txt file.

The SCCP GTT Pattern is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SCCP GTT Pattern is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNGPE:GTPID=1;

See either the individual parameter definitions or the config.txt command "STN_RSGLIST" for a full description of the parameters used in the output format.

6.3.26 CNGPI - SCCP GTT Pattern Initiate

This command adds a new SCCP GTT Pattern.

Note: SCCP GTT Patterns are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNGPI:GTPID=;

Web Management Location

System Administration > Transaction > GTT Patterns > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Pattern ID has not been initiated.

The SCCP GTT Pattern is present in the config.txt file.

There are no startup parse or configuration errors present.

The SCCP GTT Pattern is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNGPI:GTPID=1;

6.3.27 CNGPP - SCCP GTT Pattern Configuration

This command shows GTT Patterns defined on the system.

Syntax

CNGPP:[NC=,][GTPID=,];

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNGPP;

Output Format

```
SCCP GTT Pattern Configuration
GTPID     NC      AI      SPC      SSN     GT                      GTAI_PATTERN
5         NC0     0x10    0         0      0x001104                22/?6+
1023      NC1     0x10    0         0      0x001104                --/+6
```

See either the individual parameter definitions or the config.txt command "SCCP_GTT_PATTERN" for a full description of the parameters used in the output format.

6.3.28 CNGTE - SCCP GTT Translation End

This command removes an SCCP GTT Translation.

Note: SCCP GTT Translations are dynamically removed by first deleting the Gateway List from the config.txt file and then executing this command to unload the Gateway List from the system.

Syntax

CNGTE:GTPID=;

Web Management Location

System Administration > Transaction > GTT Translations > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Translation ID has been initiated.

The SCCP GTT Translation is not present in the config.txt file.

The SCCP GTT Translation is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SCCP GTT Translation is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNGTE:GTPID=1;

6.3.29 CNGTI - SCCP GTT Translation Initiate

This command adds a new SCCP GTT Translation.

Note: SCCP GTT Translations are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNGTI:GTPID=;

Web Management Location

System Administration > Transaction > GTT Translations > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SCCP GTT Translation ID has not been initiated.

The SCCP GTT Translation is present in the config.txt file.

There are no startup parse or configuration errors present.

The SCCP GTT Translation is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNGTI:GTPID=1;

6.3.30 CNGTP - SCCP GTT Translation Configuration

This command shows GTT Translations defined on the system.

Refer to the config.txt command SCCP_GTT for a full description of the parameters.

Syntax

CNGTP:[NC=,][GTPID=,];

Web Management Location

System Administration > SCCP > GTT Translations > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNGTP;

Output Format

```
SCCP GTT Translation Configuration

GTPID   NC     GTT_MASK            PRI_GTAID SEC_GTAID GTTSRC BAK_DUAL OPTIONS RIID

4       NC0    R--/K--/R           4                   ANY    N        0x0000  0

5       NC0    R-/K                5                   ANY    N        0x0000  0

1023    NC1    R-/K                1023                ANY    N        0x0000  0
```

6.3.31 CNHSP - Host Configuration

This command displays DSI Host Configuration.

Note: See the individual parameter definitions of the config.txt command SIU_HOSTS defined in the user manual for a full description of the parameters supported.

Warning: If an entry exists in config.txt then associated MMI change commands will be disabled.

Syntax

CNHSP;

Web Management Location

System Administration > DSI Hosts > Hosts > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

CNHSP;

Output Format

```
Host Configuration
  NUM_HOSTS    1
  BACKUP_HOST  BACKUP_NONE
  OPTIONS      0x00000000
  MIN_HOSTS    1
  DMHOST       0
```

See either the individual parameter definitions or the config.txt command "SIU_HOSTS" for a full description of the parameters used in the output format.

6.3.32 CNLAE - SIGTRAN Local Application Server End

This command removes an SIGTRAN Local Application Server (LAS).

Note: SIGTRAN LASs are dynamically removed by first deleting the SIGTRAN LAS from the config.txt file and then executing this command to unload the SIGTRAN LAS from the system.

Syntax

CNLAE:LAS=;

Web Management Location

System Administration > SIGTRAN > Local Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

CNLAE:LAS=1;

Prerequisites

The SIGTRAN LAS has been initiated.

The SIGTRAN LAS is not present in the config.txt file.

The SIGTRAN LAS is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN Local Application Server is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

6.3.33 CNLAI - SIGTRAN Local Application Server Initiate

This command adds a new SIGTRAN Local Application Server (LAS).

SIGTRAN LASs are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNLAI:LAS=;

Web Management Location

System Administration > SIGTRAN > Local Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN LAS has not been initiated.

The SIGTRAN LAS is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN LAS is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNLAI:LAS=1;

6.3.34 CNLAP - SIGTRAN Local Application Server Configuration

This command displays the configuration of SIGTRAN Local Application Servers on the system.

Syntax

CNLAP;

Web Management Location

System Administration > SIGTRAN > Local Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNLAP;

Output Format

```
SIGTRAN Local Application Server Configuration
LAS   NC   OPC        RC         TRMD OPTIONS LABEL
1     NC0  1200       1          LS   0x0000
2     NC1  1300       2          OR   0x0000
```

See either the individual parameter definitions or the config.txt command "STN_LAS" for a full description of the parameters used in the output format.

6.3.35 CNLCP - Software License Capability Configuration

This command shows which software licenses are available on the system.

Syntax

CNLCP;

Web Management Location

System Administration > Software > Software Licenses > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNLCP;

Output Format

```
Software License Capability Status
CAPABILITY  EVALUATION LINKS     RATE
SIU
SCTP
M2PA
M3UA          16                 154
TDM           16
```

6.3.36 CNLDE - SCCP Loadshare DPC Configuration End

The command removes aan SCCP Loadshare DPC.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command SCCP_LOAD_SHARE_DPC entry from the config.txt file.
2) Executing the CNLDE MMI command to unload it from the system.

Syntax

CNLDE:LSTSEQ=;

Web Management Location

System Administration > SCCP > Load Share Tables > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

The SCCP Loadshare DPC ID has been initiated.
The SCCP Loadshare DPC is not present in the config.txt file.
The SCCP Loadshare DPC is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The SCCP Loadshare DPC is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNLDE:LSTSEQ=1;

6.3.37 CNLDI - SCCP Loadshare DPC Configuration

This command adds a new SCCP Loadshare DPC.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, SCCP_LOAD_SHARE_DPC, in the config.txt file.
2) Executing the CNLDI MMI command to load that configuration.

Syntax

CNLDI:LSTSEQ=;

Web Management Location

System Administration > SCCP > Load Share Tables > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

The SCCP Loadshare DPC ID has not been initiated.
The SCCP Loadshare DPC is present in the config.txt file.

Example

CNLDI:LSTSEQ=1;

6.3.38 CNLDP - SCCP Loadshare DPC Configuration

This command shows the SCCP Loadshare tables defined on the system.

Syntax

CNLDP;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNLDP;

Output Format

```
SCCP Loadshare DPC Configuration
LSTSEQ      DPC
LST-5-0     2222
LST-5-1     2223
LST-6-0     1011
LST-6-1     1014
LST-6-2     1015
LST-7-0     1011
LST-7-1     1013
```

See either the individual parameter definitions or the config.txt command "SCCP_LOAD_SHARE_DPC" defined in the user manual for a full description of the parameters used in the output format.

6.3.39 CNLSE - SS7 Link Set End

This command removes an SS7 Link Set.

Note: SS7 Link Sets are dynamically removed by first deleting the SS7 Link Set from the config.txt file and then executing this command to unload the SS7 Link Set from the system.

Syntax

CNLSE:LINKSET=;

Web Management Location

System Administration > SS7 > SS7 Link Sets > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SS7 Link Set has been initiated.

The SS7 Link Set is not present in the config.txt file.

An MTP linkset cannot be removed if it contains MTP links or is used on any MTP route.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SS7 Link Set is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNLSE:LINKSET=1;

6.3.40 CNLSI - SS7 Link Set Initiate

This command adds a new SS7 Link Set.

Note: SS7 Link Sets are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNLSI:LINKSET=;

Web Management Location

System Administration > SS7 > SS7 Link Sets > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SS7 Link Set has not been initiated.

The SS7 Link Set is present in the config.txt file.

There are no startup parse or configuration errors present.

The SS7 Link Set is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNLSI:LINKSET=1;

6.3.41 CNLSP - SS7 Link Set Configuration

This command displays all configured SS7 Link Sets.

Syntax

CNLSP:[LINKSET=];

Web Management Location

System Administration > SS7 > SS7 Link Sets > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNLSP;

Output Format

```
SS7 Link Set Configuration
LINKSET  NC      OPC        APC        NLINKS SSF OPTIONS LABEL
0        NC0     1234       5678       16     0x8 0x0000
1        NC0     1234       9876       16     0x8 0x0000
```

See either the individual parameter definitions or the config.txt command "MTP_LINKSET" for a full description of the parameters used in the output format.

6.3.42 CNLTE - SCCP Loadshare Table Configuration End

The command removes aan SCCP Loadshare Table.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command SCCP_LOAD_SHARE_TABLE entry from the config.txt file.
2) Executing the CNLTE MMI command to unload it from the system.

Syntax

CNLTE:LST=;

Web Management Location

System Administration > SCCP > Load Share Tables > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

The SCCP Loadshare Table ID has been initiated.
The SCCP Loadshare Table is not present in the config.txt file.
The SCCP Loadshare Table is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The SCCP Loadshare Table is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNLTE:LST=1;

6.3.43 CNLTI - SCCP Loadshare Table Configuration

This command adds a new SCCP Loadshare Table.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, SCCP_LOAD_SHARE_TABLE, in the config.txt file.
2) Executing the CNLTI MMI command to load that configuration.

Syntax

CNLTI:LST=;

Web Management Location

System Administration > SCCP > Load Share Tables > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

The SCCP Loadshare Table ID has not been initiated.
The SCCP Loadshare Table is present in the config.txt file.

Example

CNLTI:LST=1;

6.3.44 CNLTP - SCCP Loadshare Table Configuration

This command shows the SCCP Loadshare tables defined on the system.

Selecting a particular 'ID' field on the command will result in the following associated command being executed:
`SCCP Loadshare DPC Configuration (CNLDP)`

Syntax

CNLTP;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNLTP;

Output Format

```
SCCP Loadshare Table Configuration
LST      NC    OPTIONS
LST-5    NC0   0x00000001
LST-7    NC1   0x00000003
```

See either the individual parameter definitions or the config.txt command "SCCP_LOAD_SHARE_TABLE" defined in the user manual for a full description of the parameters used in the output format.

6.3.45 CNMLE - SS7 Monitor Link End

This command removes an SS7 Monitor Link.

Note: SS7 Monitor Links are dynamically removed by first deleting the SS7 Monitor Link from the config.txt file and then executing this command to unload the SS7 Monitor Link from the system.

Syntax

CNMLE:MLINK=;

Web Management Location

System Administration > SS7 > SS7 Monitor Links > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The SS7 Monitor Link has been initiated.

The SS7 Monitor Link is not present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SS7 Monitor Link is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNMLE:MLINK=1;

6.3.46 CNMLI - SS7 Monitor Link Initiate

This command adds a new SS7 Monitor Link.

Note: SS7 Monitor Links are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNMLI:MLINK=;

Web Management Location

System Administration > SS7 > SS7 Monitor Links > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

The SS7 Monitor Link has not been initiated.

The SS7 Monitor Link is present in the config.txt file.

The SS7 Monitor Link is not used in any other configuration.

There are no startup parse or configuration errors present.

The SS7 Monitor Link is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNMLI:MLINK=1;

6.3.47 CNMLP - SS7 Monitor link Configuration

This command displays the configuration data for Monitor links

Syntax

CNMLP:[MLINK=,];

Web Management Location

System Administration > SS7 > SS7 Monitor Links > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

CNMLP;

Output Format

```
SS7 Monitor link Configuration
  MLINK IFTYPE    BPOS BLINK STREAM TS  USER_ID USER_HOST OPTIONS    VPI VCI LABEL
  0     TDM       0    1     0      16  0x1d    0         0x00000003
  1     TDM       0    2     1      16  0x1d    1         0x00000003
  2     ATM       1    1     1          0x1d    1         0x00000003 0   1
```

See either the individual parameter definitions or the config.txt command "MONITOR_LINK" for a full description of the parameters used in the output format.

6.3.48 CNMNI / CNMNE - Multi-Node Configuration

Command to dynamically initiate and end Nodes within in a Multi-Node Cluster.

To dynamically add a Node, first add a new MULTI_NODE command in the config.txt file and then execute the CNMNI command to load the configuration into the system.

To dynamically remove a Node, first remove the corresponding MULTI_NODE command from the config.txt file and then execute the CNMNE command to remove the configuration from the system.

Syntax

CNMNI:MNID=;

CNMNE:MNID=;

Web Management Location

System Administration > Server Management > Multi-Node > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Update Access

Prerequisites

There are no startup parse or configuration errors present in the alarm log.

To remove a Node it must not be in use in any other configuration.

Example

CNMNI:MNID=1;

CNMNE:MNID=1;

6.3.49 CNMNP - Multi-Node Configuration Print

This command displays the configuration data for a Node within a Multi-Node Cluster as configured using the MULTI_NODE command in config.txt.

Syntax

CNMNP:[MNID=,];

Web Management Location

System Administration > Server Management > Multi-Node > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

CNMNP;

Output Format

```
Multi-Node Configuration
MNID  MNMODE        IPHOST_NAME
0     MASTER         dsh-0015123475432
1     SEC_MASTER     dsh-0016347989540
2     GROUP_MEMBER   dsh-0012454362376
```

6.3.50 CNOBP - SNMP Trap Configuration

This command displays the configuration of SNMP Traps for all SNMP objects.

Syntax

CNOBP:[OBJGRP=;]

Web Management Location

System Administration > Diagnostics > SNMP Traps > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Prerequisites

The DSMI agent must be enabled.

All object states are set to CHANGE by default - meaning that if the state changes then a trap will be generated to all configured SNMP managers

Example

CNOBP;

Output Format

```
CNOBP:OBJGRP=5;
  SNMP Trap Configuration

  OBJIDX OBJGRP OBJECT TUP    TDOWN    TINACTIVE TIMPAIR TRESTART TQUIESCE TWARNING
    10     5      1    CHANGE  ALL     CREATE     NONE    DESTROY  CHANGE   CHANGE
    11     5      2    ALL     ALL     CHANGE     CHANGE  CHANGE   CHANGE   CHANGE
```

6.3.51 CNOBS - Configuration SNMP Traps Set

This command allows a user to determine the conditions under which an SNMP TRAP will be generated for a particular DSMI object. Essentially, a TRAP can be generated:

- When any row within an object changes state (CHANGE)
- When a new row (with a particular state) is created within an object (CREATE)
- When a row (with a particular state) is destroyed within an object (DESTROY)
- When any combination of the above occur (ALL), or when an event occurs that affects the alarm condition of the object, but does not necessarily change the state.

TRAPs can also be completely disabled (NONE).

Possible states that a DSMI object can transition into are:

UP - Operational and available

DOWN - Not available

INACTIVE - Operational but not available

IMPAIR - Operational and available but encountering service-affecting condition (e.g., congestion).

RESTART - Unavailable but will soon be available

QUIESCE - Operational but in the process of shutting down/being removed

WARNING - Operational and available but encountering a non service-affecting condition

Only one states TRAP configuration can be configured per single invocation of this command.

The CNOBP command displays the current TRAP configuration for each object.

These TRAP messages are sent to SNMP managers, which are defined with the CNSMI command. The default setting for object states is CHANGE.

Syntax

```
CNOBS:OBJGRP=,OBJECT=,[TUP=,][TDOWN=,][TINACTIVE=,][TIMPAIR=,] [TRESTART=,][TQUIESCE=,][TWARNING=,]
CNOBS:OBJIDX ,TUP=,][TDOWN=,][TINACTIVE=,][TIMPAIR=,] [TRESTART=,][TQUIESCE=,][TWARNING=,]
```

Web Management Location

System Administration > Diagnostics > SNMP Traps > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI agent must be enabled.

Only one state/trap can be specifed per command.

States can be set to CREATE, DESTROY, ALL, NONE or CHANGE

Example

CNOBS:OBJGRP=7,OBJECT=2,TDOWN=all; This will cause a TRAP to be generated whenever an SS7 link is created in the Down state, or destroyed while in the Down state or when the link enters the Down state.

6.3.52 CNPCE - PCM End

This command removes an PCM.

Note: PCMs are dynamically removed by first deleting the PCM from the config.txt file and then executing this command to unload the PCM from the system.

Syntax

CNPCE:PORTID=;

Web Management Location

System Administration > Boards > PCMs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The PCM Port has been initiated.

The PCM Port is not present in the config.txt file.

The PCM is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The PCM is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNPCE:PORTID=1;

6.3.53 CNPCI - PCM Initiate

This command adds a new PCM.

Note: PCMs are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNPCI:PORTID=;

Web Management Location

System Administration > Boards > PCMs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The PCM Port has not been initiated.

The PCM Port is present in the config.txt file.

There are no startup parse or configuration errors present.

The PCM is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNPCI:PORTID=1;

6.3.54 CNPCP - PCM Configuration

This command displays all configured PCM ports.

Syntax

CNPCP;

Web Management Location

System Administration > Boards > PCMs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNPCP;

Output Format

```
PCM Configuration
PORTID PCM LIUTYPE LC    FF   CRC_MODE  SYNCPRI BUILDOUT SLAVE OPTIONS LABEL
0      1-3 E1     HDB3  G704 NONE      0       0        0     0x0000
1      1-4 E1     HDB3  G704 NONE      0       0        0     0x0000
```

See either the individual parameter definitions or the config.txt command "LIU_CONFIG" for a full description of the parameters used in the output format.

6.3.55 CNRAE - SIGTRAN Remote Application Server End

This command removes an SIGTRAN Remote Application Server (RAS).

Note: SIGTRAN RASs are dynamically removed by first deleting the SIGTRAN RAS from the config.txt file and then executing this command to unload the SIGTRAN RAS from the system.

Syntax

CNRAE:RAS=;

Web Management Location

System Administration > SIGTRAN > Remote Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN RAS has been initiated.

The SIGTRAN RAS is not present in the config.txt file.

The SIGTRAN RAS is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN RAS is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNRAE:RAS=1;

6.3.56 CNRAI - SIGTRAN Remote Application Server Initiate

This command adds a new SIGTRAN Remote Application Server (RAS).

Note: SIGTRAN RASs are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNRAI:RAS=;

Web Management Location

System Administration > SIGTRAN > Remote Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN RAS has not been initiated.

The SIGTRAN RAS is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN RAS is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNRAI:RAS=1;

6.3.57 CNRAP - SIGTRAN Remote Application Server Configuration

This command displays the configuration of SIGTRAN Remote Application Servers on the system.

Syntax

CNRAP;

Web Management Location

System Administration > SIGTRAN > Remote Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNRAP;

Output Format

```
SIGTRAN Remote Application Server Configuration
RAS   NC   DPC        RC         NASP OPTIONS LABEL
1     NC0  2200       1          1    0x0000
2     NC1  2300       2          1    0x0000
```

See either the individual parameter definitions or the config.txt command "STN_RAS" for a full description of the parameters used in the output format.

6.3.58 CNRDI - Configuration Restore Default Initiate

This command restores the protocol configuration (config.txt) file to the original default. The file does not include any commands, but provides guidelines on how to edit the file for a real configuration.

Syntax

CNRDI;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Example

CNRDI;

6.3.59 CNRLE - SIGTRAN Remote Application Server List End

This command removes an SIGTRAN Remote Application Server list entry (RLID).

Note: SIGTRAN RLIDs are dynamically removed by first deleting the SIGTRAN RLID from the config.txt file and then executing this command to unload the SIGTRAN RLID from the system.

Syntax

CNRLE:RLID=;

Web Management Location

System Administration > SIGTRAN > Remote Server Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN RLID has been initiated.

The SIGTRAN RLID is not present in the config.txt file.

The SIGTRAN RLID is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN RLID is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNRLE:RLID=1;

6.3.60 CNRLI - SIGTRAN Remote Application Server List Initiate

This command adds a new SIGTRAN Remote Application Server List entry(RLID).

Note: SIGTRAN RLIDs are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNRLI:RLID=;

Web Management Location

System Administration > SIGTRAN > Remote Server Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN RLID has not been initiated.

The SIGTRAN RLID is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN RLIDs is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNRLI:RLID=1;

6.3.61 CNRLP - SIGTRAN Remote Application Server List Configuration

This command displays the assignment of SIGTRAN links to Remote Application Servers on the system.

Syntax

CNRLP:[RAS=],;

Web Management Location

System Administration > SIGTRAN > Remote Server Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNRLP; CNRLP:RAS=3;

Output Format

```
SIGTRAN Remote Application Server List
RLID RAS SNLINK
1    16  1
2    16  2
3    16  32
```

See either the individual parameter definitions or the config.txt command "STN_RASLIST" for a full description of the parameters used in the output format.

6.3.62 CNSBE - SIGTRAN Local Bind End

This command removes a SIGTRAN Bind.

Note: SIGTRAN binds are dynamically removed by first deleting the SIGTRAN bind from the config.txt file and then executing this command to unload the SIGTRAN bind from the system.

Syntax

CNSBE:BIND=;

Web Management Location

System Administration > SIGTRAN > Local Binds > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN Bind has been initiated.

The SIGTRAN Bind is not present in the config.txt file.

The SIGTRAN Bind is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN Bind is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNSBE:BIND=1;

6.3.63 CNSBI - SIGTRAN Local Bind Initiate

This command adds a new SIGTRAN Bind.

Note: SIGTRAN binds are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNSBI:BIND=;

Web Management Location

System Administration > SIGTRAN > Local Binds > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN bind has not been initiated.

The SIGTRAN bind is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN Bind is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNSBI:BIND=1;

6.3.64 CNSBP - SIGTRAN Local Bind Configuration

This command displays the association between the Local Application Server with the Remote Application Server or Remote Signaling Gateway, identifying the route to reach the destination.

Syntax

CNSBP;

Web Management Location

System Administration > SIGTRAN > Local Binds > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSBP;

Output Format

```
Configuration SIGTRAN Bind
BIND LAS RAS RSG OPTIONS
1    1   1       0x0000
2    2   2       0x0000
3    3      23   0x0000
4    3      21   0x0000
```

See either the individual parameter definitions or the config.txt command "STN_LBIND" for a full description of the parameters used in the output format.

6.3.65 CNSLE - SS7 Link End

This command removes an SS7 Link.

Note: SS7 Links are dynamically removed by first deleting the SS7 Link from the config.txt file and then executing this command to unload the SS7 Link from the system.

Syntax

CNSLE:LINK=;

Web Management Location

System Administration > SS7 > SS7 Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SS7 Link has been initiated.

The SS7 Link is not present in the config.txt file.

The SS7 Link has been deactivated.

The SS7 Link is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SS7 Link is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNSLE:LINK=1;

6.3.66 CNSLI - SS7 Link Initiate

This command adds a new SS7 Link.

Note: SS7 Links are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNSLI:LINK=;

Web Management Location

System Administration > SS7 > SS7 Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SS7 Link has not been initiated.

The SS7 Link is present in the config.txt file.

There are no startup parse or configuration errors present.

The SS7 Link is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNSLI:LINK=1;

6.3.67 CNSLP - SS7 Link Configuration

This command displays the configuration data for SS7 signaling links.

Syntax

CNSLP:[LINK=,];

Web Management Location

System Administration > SS7 > SS7 Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSLP;

Output Format

```
SS7 Link Configuration
LINK LINKSET REF SLC BPOS BLINK STREAM TS  OPTIONS      IFTYPE  VPI VCI LABEL
0    1       0   0   1    0     0      1   0x00000006    TDM
1    1       1   1   1    1     0      2   0x00000006    TDM
2    1       2   2   1    2     0      3   0x00000006    TDM
3    1       3   3   1    3     0      4   0x00000006    TDM
4    1       3   3   1    1     1          0x00000006    ATM    0   1
```

See either the individual parameter definitions or the config.txt command "MTP_LINK" for a full description of the parameters used in the output format.

6.3.68 CNSMC - Configuration SNMP Manager Change

This command allows changes to the configured SNMP Manager. For SNMP v3 TRAPs, an engine identifier can be optionally specified for use with a particular remote SNMP manager. The engine identifier is configured with the ENGINE parameter. If an ENGINE identifier is not specified, then the system will use its default ENGINE identifier (the value of which can be auto discovered and can be viewed using the SNMP Configuration command). For most use cases, the default ENGINE identifier should be used rather than configuring an explicit ENGINE ID with this command.

Syntax

CNSMC:MNGR=,[IPADDR=,][TPORT=,][TFORMAT=,][TCOM=,][SNMPUSER=,][ENGINE=,][LABEL=;]

Web Management Location

System Administration > Diagnostics > SNMP Managers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI agent must be enabled.

The manager must be configured.

If an SNMP V3 user is specified, the user must already be defined.

Engine can only be specified if the user is set or has been previously set.

TFORMAT can only be set to a value other than NONE if the user and engine are not set.

TFORMAT must be set to NONE if the user is set.

A manager cannnot be changed to or from SNMP V3.

Example

```
CNSMC:MNGR=1,ENGINE=0a0bccff110d0e99;
```

6.3.69 CNSME - Configuration SNMP Manager End

This command removes SNMP manager configuration.

Syntax

CNSME:MNGR=;

Web Management Location

System Administration > Diagnostics > SNMP Managers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI agent must be enabled.

The manager must be configured.

6.3.70 CNSMI - Configuration SNMP Manager Initiate

This command allows the administrator to define up to 32 TRAP destinations (i.e., remote SNMP manager stations). Each manager is defined by its IP address Additionally, the type of TRAP to be dispatched to the SNMP manager is specified with the Trap Format parameter.

The port parameter allows configuration of a destination port which is different from the default standard SNMP TRAP port (162).

If the remote SNMP (v1 or v2c) manager has been configured to only recognize TRAPs received with a community string, the TCOM parameter accommodates that value.

If an SNMP v3 TRAP is to be issued, then the USER parameter value is used. The USER parameter is used to specify a user, which has been defined with the CNUSI command. For SNMP V3 TRAPs, an engine identifier can be optionally specified for use with a particular remote SNMP manager. The engine identifier is configured with the ENGINE parameter. If an ENGINE identifier is not specified, then the system will use its default ENGINE identifier (the value of which can be auto discovered and viewed using the SNMP Configuration command). For most use cases, the default ENGINE identifier should be used rather than configuring an explicit ENGINE ID with this command.

Finally, the LABEL parameter is used to specify an optional string identifier for the manager.

Syntax

CNSMI:MNGR=,IPADDR=,[TPORT=,][TFORMAT=,][TCOM=,][SNMPUSER=,][ENGINE=,][LABEL=,];

Web Management Location

System Administration > Diagnostics > SNMP Managers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI agent must be enabled.

If a USER is specified, the USER must be configured.

If an ENGINE is specified the USER must also be specified.

If USER is specified then TFORMAT should be set to NONE.

If USER is not specified then TFORMAT cannot be set to NONE.

Example

This is an example for setting up a simple SNMP v2 TRAP receiver/manager:

CNSMI:MNGR=1,IPADDR=192.168.1.22,TFORMAT=V2TRAP;

This next example shows the creation of a SNMP v3 TRAP receiver/manager.

The first step is to define the user with the CNUSI command:

CNUSI:USER=1,AUTH=MD5,AUTHPASS=abcdefgh,LABEL=user1;

The next step is to define the manager which references the user which has just been defined:

CNSMI:MNGR=2,IPADDR=192.168.1.222,TFORMAT=NONE,USER=1,

6.3.71 CNSMP - SNMP Manager Configuration

This commands displays configuration of SNMP Managers

Syntax

CNSMP:[MNGR=;]

Web Management Location

System Administration > Diagnostics > SNMP > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Prerequisites

Prerequisites: If specified the manager must be configured.

Example

CNSMP; CNSMP:MNGR=4;

Output Format

```
SNMP Manager Configuration
MNGR IPADDR          TPORT TFORMAT TCOM      SNMPUSER ENGINE               LABEL
1    192.168.0.27    162   V2TRAP  public    0                            mngr1
2    192.168.1.77    162   NONE    public    2        0a0b0c0d0e0f1234    mngr2
```

6.3.72 CNSNP - SNMP Configuration

This command displays the configuration of the SNMP agent.

The DFLT_ENGINE identifier shown is the default SNMP V3 ENGINE identifier for use with SNMP V3 traps. If an SNMP manager is not configured on the system with an explicit ENGINE identifier, then this identifier will be used when sending SNMP V3 traps.

The DSMIEVENT identifier determines the type of SNMP notifications that are sent by the system.

Syntax

CNSNP;

Web Management Location

System Administration > Diagnostics > SNMP > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSNP;

Output Format

```
SNMP Configuration

SNMP         Y

RCOM         public

DFLT_ENGINE 80001f8880e313894fdcdecb520000

DSMIEVENT    OBJECT
```

6.3.73 CNSNS - Configuration SNMP Set

This command allows the configuration of the SNMP agent to be modified.

For the SNMP parameter to take effect, a system restart is required.

Syntax

CNSNS:SNMP=;

CNSNS:RCOM=;

Web Management Location

System Administration > Diagnostics > SNMP > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

CNSNS:SNMP={Y|N};

CNSNS:RCOM=public;

CNSNS:DSMIEVENT=OBJECT;

6.3.74 CNSRE - SIGTRAN Route End

This command removes an SIGTRAN route.

Note: SIGTRAN routes are dynamically removed by first deleting the route from the config.txt file and then executing this command to unload the route from the system.

Syntax

CNSRE:SNRT=;

Web Management Location

System Administration > SIGTRAN > Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN Route ID has been initiated.

The SIGTRAN Route is not present in the config.txt file.

The SIGTRAN Route is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN route is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNSRE:SNRT=1;

6.3.75 CNSRI - SIGTRAN Route Initiate

This command adds a new SIGTRAN route.

Note: SIGTRAN routes are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNSRI:SNRT=;

Web Management Location

System Administration > SIGTRAN > Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN Route ID has not been initiated.

The SIGTRAN Route is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN route is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNSRI:SNRT=1;

6.3.76 CNSRP - SIGTRAN Route Configuration

This command displays the configuration of SIGTRAN routes.

Syntax

CNSRP;

Web Management Location

System Administration > SIGTRAN > Routes > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSRP;

Output Format

```
SIGTRAN Route Configuration
SNRT  NC      DPC       OPTIONS LABEL
1     NC3     401       0x0000
41    NC3     1019      0x0000
```

See either the individual parameter definitions or the config.txt command "STN_ROUTE" for a full description of the parameters used in the output format.

6.3.77 CNSSE - SCCP Subsystem Resource End

This command removes an Sub-System Resource.

Note: Sub-System Resources are dynamically removed by first deleting the Resource from the config.txt file and then executing this command to unload the Resource from the system.

Syntax

CNSSE:SSRID=;

Web Management Location

System Administration > Transaction > SCCP SSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The Sub-System Resource has been initiated.

The Sub-System Resource is not present in the config.txt file.

The Sub-System Resource is not used in any other configuration.

Local Sub-System Resources other than SCCP cannot be dynamically removed.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The Sub-System Resource is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNSSE:SSRID=1;

6.3.78 CNSSI - SCCP Subsystem Resource Initiate

This command adds a new Sub-System Resource.

Note: Sub-System Resources are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNSSI:SSRID=;

Web Management Location

System Administration > Transaction > SCCP SSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The Sub-System Resource ID has not been initiated.

The Sub-System Resource is present in the config.txt file.

There are no startup parse or configuration errors present.

The Sub-System Resource is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNSSI:SSRID=1;

6.3.79 CNSSP - SCCP Subsystem Resource Configuration

This command displays SSR configuration data.

Syntax

CNSSP:[SSRID=],[SSR=],[NC=];

Web Management Location

System Administration > Transaction > SCCP SSRs > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSSP;

Output Format

```
SCCP Subsystem Resource Configuration
SSRID  NC  SSR SPC      SSN USER_ID OPTIONS PCMASK     LSSPROT  RIID  LABEL
1      NC0 LSS             8     0x1d       0x00000                  MAP
2      NC0 RSP 16381                        0x00000    0x00000000               0      To_SGW_RSP
```

See either the individual parameter definitions or the config.txt commands "SCCP_LSS", "SCCP_RSS" and "SSCP_RSP" for a full description of the parameters used in the output format.

6.3.80 CNSTE - SIGTRAN Link End

This command removes an SIGTRAN link.

Note: SIGTRAN links are dynamically removed by first deleting the SIGTRAN link from the config.txt file and then executing this command to unload the SIGTRAN link from the system.

Syntax

CNSTE:SNLINK=;

Web Management Location

System Administration > SIGTRAN > Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN link has been initiated.

The SIGTRAN link is not present in the config.txt file.

The SIGTRAN link is not used in any other configuration.

There are no restart or configuration failed alarms present in the alarm log.

There are no startup parse or configuration errors present.

The SIGTRAN link is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

CNSTE:SNLINK=1;

6.3.81 CNSTI - SIGTRAN Link Initiate

This command adds a new SIGTRAN link.

Note: SIGTRAN links are dynamically added by first adding the configuration to the config.txt file and then executing this command to load that configuration onto the system.

Syntax

CNSTI:SNLINK=;

Web Management Location

System Administration > SIGTRAN > Links > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The SIGTRAN link has not been initiated.

The SIGTRAN link is present in the config.txt file.

There are no startup parse or configuration errors present.

The SIGTRAN link is present in the config.txt file.

There are no restart or configuration failed alarms present in the alarm log.

Example

CNSTI:SNLINK=1;

6.3.82 CNSTP - SIGTRAN Link Configuration

This command displays the configuration of SIGTRAN links.

Syntax

CNSTP:[SNLINK=,][SNTYPE=][PAGE=];

Web Management Location

System Administration > Software > System Software > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSTP;

Output Format

```
SIGTRAN Link Configuration (Page 1 of 2)
  SNLINK  SNTYPE RIP1            RIP2             LIP1            LIP2    LABEL
  1       M3UA   10.22.131.1     10.22.131.2

SIGTRAN Link Configuration (Page 2 of 2)
  SNLINK  SNTYPE END LPORT RPORT OPTIONS  M2PA ID RSG NC   NA    LABEL
  1       M3UA   C   3565 3565   0x0000               NC0
```

See either the individual parameter definitions or the config.txt command "STN_LINK" for a full description of the parameters used in the output format.

6.3.83 CNSWP - System Software Configuration

This command displays the version of active software, and if applicable the previous software version. It also lists and software available for other operating modes.

Syntax

CNSWP;

Web Management Location

System Administration > Software > System Software > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSWP;

Output Format

```
  System Software Configuration
  SYSTYPE     SIU
  RESTART     SOFT
  RESET       N
  OPERATING   SS7G40-SIU Release 1.0.0 (Build 1001)
```

6.3.84 CNSYP - System Configuration

This command displays the system configuration including the system identity, contact and system location details as well as proving information on diagnostic trace management.

Syntax

CNSYP;

Web Management Location

System Administration > Server Management > System > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNSYP;

New row between UNITID and SYSID with the text

UNIT_SERIAL LG401002

The spacing should be the same as that for other rows.

Output Format

```
SS7G40(SIU)     System Configuration
UNITID          0014b2a2ee2c
NODE            sysnode
SYSID           normal system_id
SYSREF          0
CONTACT         acontact@address.com
LOCATION        normal location
LEDID           N
TRACELOG        DUAL
TRACEFMT        DUAL
TDMSHARE
M3UASHARE       50
LINES           0
TLO             30
DEBUG           N
```

6.3.85 CNSYS - Configuration System Set

This command changes the system level parameters.

Syntax

CNSYS:{[NODE=,][SYSID=,][SYSREF=,][CONTACT=,][LOCATION=,][LINES=,][TLO=,][DSE=,]

[LEDID=,][TRACELOG=,][TRACEFMT=,][TDMSHARE=,][M3UASHARE=,][IPDISPLAY=,]};

Web Management Location

System Administration > Server Management > System > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

DSE can only be activated if the SDP license is present.

Cannot set TRACELOG to host or dual if there is no management host.

Example

CNSYS:SYSID=Wilma;

6.3.86 CNTDP - Time and Date Configuration

This command displays out the system date and time, whether NTP is active and to display the OFFSET from UTC configured changes.

Syntax

CNTDP;

Web Management Location

System Administration > Server Management > System Time > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNTDP;

Output Format

```
Time and Date Configuration
DATE   2001-10-03
TIME   09:04:02
NTP    Y
OFFSET +5:30
```

6.3.87 CNTDS - Configuration Time and Day Set

This command specifies the date and time as used by the system. This command can also activate or deactivate Network Time Protocol (NTP) on the system. System time is used to indicate the time an alarm occurred or cleared and to provide timestamps for such things as measurements and data records. The command also allows an OFFSET from UTC to be specified to allow the system to report the correct local time, when synchronized with a NTP time server.

Note: The system will not automatically adjust for daylight savings time changes. The system must be restarted in order for the new OFFSET value to take effect. If the OFFSET parameter is not changed there is no need to restart the system after performing a change to the configuration of Day or Time. Any subsequent requests for system restart after changing the Day or Time will, however, always result in the system performing a 'Hard' restart even if a 'Soft' one was requested. A 'Hard' restart is required to allow the systems license manager to re-sync with the new date/time.

Syntax

CNTDS:[DATE=,][TIME=][NTP=,][OFFSET=];

Web Management Location

System Administration > Server Management > System Time > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Administration Access

Example

CNTDS:DATE=2001-10-03,TIME=18:32:21,NTP=Y,OFFSET=+5:30;

6.3.88 CNTMP - Trace Masks Configuration

This command displays the current trace masks and whether or not the tracing is enabled.

Syntax

CNTMP;

Web Management Location

System Administration > Diagnostics > Trace > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNTMP;

Output Format

```
MODULE IMASK      OMASK      MMASK      ACTIVE
MTP    0x00000001 0x00000001 0x0001fffe N
ISUP   0x00000001 0x00000001 0x00000038 Y
```

6.3.89 CNTMS - Configuration Trace Mask Set

This command activates or deactivates tracing of different protocols and sets the associated trace masks. Configured values are maintained after system reset. The IMASK, OMASK, and MMASK parameters determine which Input, Output or Management messages are traced by the module. Default IMASK, OMASK, or MMASK values are restored using the "DEFAULT" token.

Note: Definitions of the IMASK, OMASK and MMASK trace mask parameters for a specific protocol are documented in the associated protocol programmer's manual.

By default, when tracing is activated on the SIU messages are logged to file in the "syslog" subdirectory of the siuftp account. This log is maintained as a rolling log of up to tem 5MB files containing trace messages. The most recent trace log file will have the name trace.log the next most recent trace.log.1 and then trace.log.2 and so on.

A user may change the destination of trace messages through use of the TRACELOG parameter on the system configuration command. A user also can select either that messages are logged to FILE (default), HOST, where they are transmitted to the management module id on the configured management host, or DUAL where they are both logged to file and sent to host.

MTP3 and M3UA traces may also be logged in PCAP file format. In a similar manner to the above text log files the system supports up to ten, 5MB PCAP log file named trace.pcap, trace.pcap.1, trace.pcap.2 etc. storing them in the syslog subdirectory of the siuftp account. Logging in TEXT or PCAP format is selected by using the TRACEFMT parameter in the CNSYx MMI command.

Activation of tracing under high load conditions may reduce overall throughput of the SIU.

Syntax

CNTMS:MODULE={[IMASK=,][OMASK=,][MMASK=,][ACTIVE=]};

Web Management Location

System Administration > Diagnostics > Trace > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

CNTMS:MODULE=ISUP,IMASK=1,OMASK=2,MMASK=3; CNTMS:MODULE=ISUP,ACTIVE=Y; CNTMS:MODULE=ISUP,ACTIVE=N; CNTMS:MODULE=ISUP,IMASK=DEFAULT;

Prerequisites

The protocol should be licensed and active before attempting to configure a trace mask for it.

6.3.90 CNTPE - Configuration Network Time Protocol Server End

This command removes a specified Network Time Protocol Server from the configuration.

Syntax

CNTPE:NTPSER=;

Web Management Location

System Administration > Server Management > NTP Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

CNTPE:NTPSER=1;

6.3.91 CNTPI - Configuration Network Time Protocol Server Initiate

This command adds a specified Network Time Protocol Server to the configuration of the system. The NTP service should be activated using the Configuration Time and Date Set command.

Syntax

CNTPI:NTPSER=,IPADDR=,[LABEL=];

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

CNTPI:NTPSER=1,IPADDR=192.168.0.1,LABEL=Primary NTP Server;

6.3.92 CNTPP - NTP Server Configuration

This command displays the configuration of the Network Time Protocol software.

Syntax

CNTPP;

Web Management Location

System Administration > Server Management > NTP Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

CNTPP;

Output Format

```
NTP Server Configuration
NTPSER IPADDR          LABEL
1      192.168.0.1     Primary NTP server
2      192.168.0.2     NTP server 2
```

6.3.93 CNURC - Configuration Update Resources Change

This command changes the configuration data or a resource on the server. The operation involves reading the config.txt file containing configuration data, validating it and applying it to the unit.

Note: Use of the CNURE command has been deprecated. Individual objects such as circuit groups and routes have their own specific commands to remove and then add modified resources to the system.

Syntax

CNURC:UPMODE=CGRP,ID=;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

The command will succeed only if the resource data is present in the updated configuration FILE and a valid configuration has been entered.

Example

CNURC:UPMODE=CGRP,ID=2;

6.3.94 CNURE - Configuration Update Resources End

This command removes the configuration of a specific resource. The operation involves reading the config.txt file containing configuration data, validating that the resource is no longer present and removing the resource from the configuration on the unit.

Note: Use of the CNURE command has been deprecated. Individual objects such as circuit groups and routes have their own specific commands to remove resources from the system.

Syntax

CNURE:UPMODE=CGRP,ID=;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

The command succeeds only if the resource data is not present in the updated configuration file, the specified circuit group was previously configured and in an INACTIVE state.

Example

CNURE:MODE=CGRP,ID=8;

6.3.95 CNURI - Configuration Update Resources Initiate

This command updates the configuration data of a resource on the server. The operation involves reading the config.txt file containing configuration data, validating it and applying it to the unit.

Note: Use of the CNURI command has been deprecated. Individual objects such as circuit groups and routes have their own specific commands to add resources to the system.

Syntax

CNURI:MODE=CGRP,ID=;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

Ensure that the appropriate resource data is present in the updated

Valid configuration has been entered.

The specified resource was not previously configured in the unit.

Example

CNURI:MODE=CGRP,ID=5;

6.3.96 CNUSC - Configuration SNMP User Change

This command allows changes to configured SNMP user accounts

Syntax

CNUSC:[SNMPUSER=,]{[AUTH=,][AUTHPASS=,][PRIV=,][PRIVPASS=][LABEL=,]}

Web Management Location

System Administration > Diagnostics > SNMP Users > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

This DSMI Agent must be enabled.

The user must be configured.

If AUTH is specifed the AUTHPASS must be provided. If PRIV is specified then PRIVPASS must be provided.

PRIV and PRIVPASS cannot be specified if AUTH and AUTHPASS are not already specified.

Example

CNUSC:SNMPUSER=1,PRIV=DES,PRIVPASS=aBcDeFgHiJkL;

The following example will remove AUTH and AUTHPASS:

CNUSC:SNMPUSER=1,AUTH=;

6.3.97 CNUSE - Configuration SNMP User End

This command removes a user account configuration.

Syntax

CNUSE:[SNMPUSER=;]

Web Management Location

System Administration > Diagnostics > SNMP Users > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI Agent must be enabled. The user must be configured.

Example

CNUSI:SNMPUSER=1;

6.3.98 CNUSI - Configuration SNMP User Initiate

This command allows configuration of up to 32 SNMP V3 user accounts. This command also allows the administrator to define SNMP v3 user accounts for use in conjunction with SNMP v3 TRAP destinations/managers. A user is defined with an integer user identifier, optional authentication and a label, which serves as the username. The user and label parameters are mandatory. Supported AUTH values are SHA and MD5. The password must have a minimum length of 8 characters, and a maximum length of 24 is enforced. The AUTH and AUTHPASS parameters must be specified together. It is not possible to configure an AUTHPASS value without having also specified the AUTH value.

Syntax

CNUSI:[SNMPUSER=,]{[AUTH=,][AUTHPASS=,][PRIV=,][PRIVPASS=][LABEL=,]}

Web Management Location

System Administration > Diagnostics > SNMP Users > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The DSMI Agent must be enabled.

If AUTH is specified, the AUTHPASS must be provided. If PRIV is specified, then PRIVPASS must be provided. PRIV and PRIVPASS cannot be specified if AUTH and AUTHPASS are not already specified.

Example

CNUSI:SNMPUSER=1,AUTH=MD5,AUTHPASS=aBcDeFgHiJkL,LABEL=user1

6.3.99 CNUSP - SNMP User Configuration

This commands displays configuration of SNMP V3 User Accounts.

Syntax

CNUSP:[SNMPUSER=;]

Web Management Location

System Administration > Diagnostics > SNMP Users > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Prerequisites

If specified the user must be configured.

Example

CNUSP:SNMPUSER=3; CNUSP;

Output Format

```
CNUSP;
SNMP User Configuration
SNMPUSER  AUTH  AUTHPASS  PRIV  PRIVPASS  LABEL
1         MD5   ********  DES   ********  user1
2         NONE            NONE            user2
```

6.4 Database Commands

"DBSVP - Subscriber Database Service Configuration"

"DBSVS – Subscriber Database Service Change"

6.4.1 DBSVP - Subscriber Database Service Configuration

This command displays the configuration associated with Subscriber Database Services.

Syntax

DBSVP;

Web Management Location

System Administration > Subscriber Database > Services > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

DBSVP;

Output Format

```
Subscriber Database Service Configuration
  DBSVCID         0
  DBSVCTYPE       MNP
  DBSVCNAME       DSILNP
  OPTIONS         0x00000000
  RETRIES         1
  RECOVERY        CONTINUE
  TESTMSISDN      123456789
  DB0             0-PRI
  DB1             3-PRI
  DB2             4-PRI
  DB3             5-PRI
  DB6             1-SEC
  DB7             2-SEC
```

6.4.2 DBSVS – Subscriber Database Service Change

This command updates a specific Database service.

The DBSVCTYPE is the type of database service and must be set to MNP, the DBSVCNAME is the actual service name for the database and the TESTMSISDN identifies the test MSISDN that is present in the MNP database and is used to validate operation of the MNP service. The RETRIES parameter indicates number database retries to attempt before declaring failure and the RECOVERY parameter identifies the recovery mechanism to use should a database lookup fail.

DB0 .. DB15 identifies the hosts used for connectivity to the database. Each host is identified in a compound parameter of the form x-y where x is the Host ID and y is set to either PRI or SEC to determine the intended usage of the host

Note: If a the number of retries allowed is set to a value equal to or greater than the number of hosts associated with Database services the system will treat this as a value of one less than the number of hosts configured.

Syntax

DBSVS:DBSVCID=,[DBSVCTYPE=,][DBSVCNAME=,][OPTIONS=,][RETRIES=,][RECOVERY=,][TESTMSISDN=,]

[DB0=,][DB1=,][DB2=,][DB3=,]

[DB4=,][DB5=,][DB6=,][DB7=,]

[DB8=,][DB9=,][DB10=,][DB11=,]

[DB12=,][DB13=,][DB14=,][DB15=,];

DBSVS:DBSVCID=,DBSVCTYPE=NONE;

Web Management Location

System Administration > Subscriber Database > Services > Configuration

Applicability

Operating Modes: SIU

Permissions: Configuration Update Access

Prerequisites

Upon change the service name and test MSISDN must be set to non null values.

If the database service type is set to a value other than NONE, then at least one database instance must be configured.

The host identified in the host sequence must exist.

The database ID must be less than the number of configured hosts.

The subscriber DB cannot be set to a host ID already associated with a management host.

If the service type is set to none, then the service is removed (and no further parameters can be set).

Example

DBSVS:DB0=0-PRI;

6.5 Helix Commands

“HDPRP - Diameter Peer Configuration”

“HMFES - Flow Environment Configuration”

“HMFEP - Flow Environment Configuration”

6.5.1 HDPRP - Diameter Peer Configuration

This command displays Diameter peer configuration data.

Syntax

HDPRP:[HDPR=];

Web Management Location

System Administration > Diameter > Peer > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

HDPRP;

HDPRP:HDPR=0;

Output Format

```
Diameter Peer Configuration
HDPR    HOST                          REALM         LABEL
0       dmr02.01.forlab.dialogic.com dialogic.com London001
1       dmr02.02.forlab.dialogic.com dialogic.com London002
2       dmr02.03.forlab.dialogic.com dialogic.com London003
3       dmr02.04.forlab.dialogic.com dialogic.com London004
```

6.5.2 HMFES - Flow Environment Configuration

This command sets the Flow Environment log and trace levels.

Syntax

HMFES,TRACELVL=,LOGLVL=;

Web Management Location

System Administration > Diagnostics > Flow Environment > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Update Access

Example

```
HMFES,TRACELVL=4,LOGLVL=4;
```

6.5.3 HMFEP - Flow Environment Configuration

This command displays configuration of the Flow Environment.

Syntax

HMFEP;

Web Management Location

System Administration > Diagnostics > Flow Environment > Configuration

Applicability

Operating Modes: DSH

ermissions: Configuration Read Access

Example

HMFEP;

Output Format

```
Flow Environment Configuration
TRACELVL        4
LOGLVL          4
```

6.6 IP Commands

"IPFWC - IP Firewall Change"

"IPFWE - IP Firewall End"

"IPFWI - IP Firewall Initiate"

"IPFWP - IP Firewall Configuration"

"IPGWE - IP Gateway End"

"IPGWI - IP Gateway Initiate"

"IPGWP - IP Gateway Configuration"

"IPLGE - IP Log End"

"IPLGI - IP Log Initiate"

"IPLGP - IP Log Configuration"

"IPNIC - IP Network Interface Configuration Change"

"IPNIE - IP Network Interface Configuration End"

"IPNII - IP Network Interface Configuration"

"IPNIP - Network Interface Configuration"

"IPHNTKE - IP Host NameToken Configuration End"

“IPHNIPTKI - IP Host NameToken Configuration”

“IPHNIPTKP - IP Host NameToken Configuration”

“IPWSP - IP Web Server Configuration”

“IPWSS - Configuration Web Service Set”

6.6.1 IPFWC - IP Firewall Change

This command changes the action taken for an IP address or network accessing the System.

Syntax

IPFWC:IPFW=,IPACT=;

Web Management Location

System Administration > Access Control > Firewall > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Security Access

Prerequisites

The IP Firewall ID has been initiated.

Example

IPFWC:IPFW=DEFAULT,IPACT=DROP;

6.6.2 IPFWE - IP Firewall End

This command disables an IP address or network from accessing the System.

Syntax

IPFWE:IPFW=;

Web Management Location

System Administration > Access Control > Firewall > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Security Access

Prerequisites

The IP Firewall ID has been initiated.

The default rule cannot be deleted.

Example

IPFWE:IPFW=1;

6.6.3 IPFWI - IP Firewall Initiate

This command defines a rule for an IP address or network accessing the System.

Syntax

IPFWI:IPFW=,IPACT=,MASK=,{IPSRC=,|IPDEST=,}[IPSVC=,];

Web Management Location

System Administration > Access Control > Firewall > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Security Access

MMI Prerequisites

The IP Firewall ID has not been initiated.
There must be at least one IPSRC or IPDEST.
If IPSRC and IPDEST are specified they must be of the same IP type (IPV4 or IPV6).

Example

IPFWI:IPFW=1,IPACT=ACCEPT,IPSRC=172.16.1.0/24;

6.6.4 IPFWP - IP Firewall Configuration

This command displays IP addresses and networks that may access the System. If no value is shown then the server may be accessed from any network that can route to it.

Note: The default IP Firewall ID cannot be deleted. This rule is the default action to be performed when no match is made by any of the other rules.

Syntax

IPFWP:[IPFW=];

Web Management Location

System Administration > Access Control > Firewall > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Prerequisites

If specified, the IP Firewall ID must have been initiated.

Example

IPFWP;

Output Format

```
IPFW    IPACT  IPSVC     IPSRC                                    IPDEST
DEFAULT DROP              ANY                                      ANY
1       ACCEPT ALL        172.16.44.0/24                           ANY
2       ACCEPT SCTP       175.21.5.5/24                            ANY
```

6.6.5 IPGWE - IP Gateway End

This command removes an IP route via an IP gateway.

Syntax

IPGWE:IPGW=;

Web Management Location

System Administration > Server Management > IP Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Prerequisites

The IP gateway id has been initiated.

Example

IPGWE:IPGW=1;

6.6.6 IPGWI - IP Gateway Initiate

This command allows the user to specify a route via an IP gateway.

Syntax

IPGWI:IPGW=,GATEWAY=,[IPNW=,];

Web Management Location

System Administration > Server Management > IP Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MWI Prerequisites

The IP gateway ID has not been initiated.
The IP Mask and and IP Network are mandatory for non default gateways.
Two gateways cannot have overlapping IP addresses.

Example

IPGWI:IPGW=2,GATEWAY=192.168.1.1,IPNW=172.16.1.0/24;
IPGWI:IPGW=1,GATEWAY=192.168.1.1,IPNW=DEFAULT;

6.6.7 IPGWP - IP Gateway Configuration

This command displays routes vian IP gateways.

Syntax

IPGWP:[IPGW=];

Web Management Location

System Administration > Server Management > IP Gateways > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Prerequisites

If the IP gateway ID is specified it must already have been initiated.

Example

IPGWP;

Output Format

```
IPGW    GATEWAY           IPNW
0       172.28.148.1/24   DEFAULT
1       192.168.1.1/24    172.16.1.0
```

6.6.8 IPLGE - IP Log End

This command removes a rule to log specific IP data.

Syntax

IPLGE:IPLG=;

Web Management Location

System Administration > Diagnostics > IP Log > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Security Access

Prerequisites

The IP Log ID has been initiated.

Example

IPLGE:IPLG=1;

6.6.9 IPLGI - IP Log Initiate

This command defines a rule to log specific IP data.

Syntax

IPLGI:IPLG=,LGTYPE=,[LGDATA=,];

Web Management Location

System Administration > Diagnostics > IP Log > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Security Access

Prerequisites

The IP Log ID has not been initiated.

Example

IPLGI:IPLG=1,LGTYPE=SCTP

6.6.10 IPLGP - IP Log Configuration

This command displays display the type of data being output to the IP log.

Syntax

IPLGP;

Web Management Location

System Administration > Diagnostics > IP Log > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

IPLGP;

Output Format

```
IPLG    LGTYPE  LGDATA
1       SCTP
```

The following is the meaning of each field:

IPLG - IP Log Identifier.

LGTYPE - The type of IP logging to be done.

LGDATA - data associated with the type.

6.6.11 IPNIC - IP Network Interface Configuration Change

This command changes the configuration of a Network Interface Device.

One IPV4 address and one IPV6 Address may be configured. The IP Address should be specified in CIDR format with IP Address and subnet mask specified as a compound parameter separated by a '/' character.

The System supports resilient IP connectivity and a bond of two Ethernet Ports may be configured. A bonding team is assigned by adding a bonding Network Interface and the assigning two Ethernet Ports to it by setting the BOND parameter on each Ethernet port using the Network Interface Change command. The MAC address of the lower numbered Ethernet port will be used as the MAC address of the bond.

If the first port fails then the second port will take over. If the first port returns to service the secondary port will remain the active port unless it in turn fails at which point the first port will resume active control of connectivity for the IP address.

Note: Ethernet Ports numbered greater than 4 can only be used when additional Network Interface Boards have been fitted.

Syntax

IPNIC:NETIF=,IP4ADDR=;
IPNIC:NETIF=,IP6ADDR=;
IPNIC:NETIF=,BOND=;

Web Management Location

System Administration > Server Management > Network Interfaces > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

Up to 2 Ethernet Ports can be in a bonding team.
Cannot associated an Ethernet port with an Bonding Network Interface if that Bonding Network Interface is not configured.
A Ethernet port cannot be a member of a bonding team if it has an IP address associated with it.
Cannot change an IP Address that is in use elsewhere (e.g., by an SCTP Association).
A bond cannot be assigned an IPV6 IP address.

Example

IPNIC:NETIF=ETH2,IP4ADDR=192.168.0.1/24;
IPNIC:NETIF=BOND0,IP4ADDR=10.1.1.10/30;
IPNIC:NETIF=ETH2,BOND=BOND0;

6.6.12 IPNIE - IP Network Interface Configuration End

This command removes a Network Interface.

Syntax

IPNIE:NETIF=;

Web Management Location

System Administration > Server Management > Network Interfaces > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

Only bonding Network Interfaces may be removed.
Cannot remove an Bonding Network interface if it associated with a
Ethernet port Network Interface.
Cannot remove an Network interface if one of its IP Addresses are in use elsewhere (e.g., by an SCTP Association).

Example

IPNIE:ETH=2;

6.6.13 IPNII - IP Network Interface Configuration

This command adds a Network Interface.

Only bonding network interfaces may be added.

One IPV4 address and one IPV6 Address may be configured. The IP Address should be specified in CIDR format with IP Address and subnet mask specified as a compound parameter separated by a '/' character.

The System supports resilient IP connectivity and a bond of two Ethernet ports may be configured. A bonding team is assigned by adding a bonding Network Interface and the assigning two Ethernet Ports to it by setting the BOND parameter on each Ethernet port using the Network Interface Change command. The MAC address of the lower numbered Ethernet port will be used as the MAC address of the bond. If the first port fails then the second port will take over. If the first port returns to service the secondary port will remain the active port unless it in turn fails at which point the first port will resume active control of connectivity for the IP address.

Syntax

IPNII:NETIF=,[IP4ADDR=,][IP6ADDR=,];

Web Management Location

System Administration > Server Management > Network Interfaces > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

Example

IPNII:NETIF=ETH0,IP4ADDR=192.168.0.1/24;

6.6.14 IPNIP - Network Interface Configuration

This command shows the IP configuration of each network interface.

Syntax

IPNIP:[NETIF=];

Web Management Location

System Administration > Server Management > Network Interfaces > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Output Format

```
IPNIP;
IP Interface Configuration
NETIF   LABEL
BOND0   Management
ETH0
ETH1
ETH2
ETH3

IPNIP:NETIF=ETH3;
IP Interface Device Configuration
NETIF      ETH3
IP4ADDR    172.28.148.126/24
IP6ADDR    fd77:19a9:8cf0:148:20e:cff:fec7:4b34/64
BOND       NONE
LABEL      Sigtran
```

6.6.15 IPHNTKE - IP Host NameToken Configuration End

This command removes configuration related to an IP Host.Token.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command IP_TOKEN entry from the config.txt file.
2) Executing the IPHNTKE MMI command to unload it from the system.

Syntax

IPHNIPTKE: IPTOKEN =;

Web Management Location

System Administration > Server Management > IP HostTokens Names > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

The IP token has been initiated.

Example

IPHNIPTKE:IPTOKEN=1;

6.6.16 IPHNIPTKI - IP Host NameToken Configuration

This command adds configuration related to an IP HostToken.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, IP_TOKEN, in the config.txt file.
2) Executing the IPHNIPTKI MMI command to load that configuration.

Syntax

IPHNIPTKI: IPTOKEN=;

Web Management Location

System Administration > Server Management > IP Host NamesTokens > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

MMI Prerequisites

There cannot be duplicate entries for an IP token and IP address.
The IPTOKEN cannot be a valid IP Addresses.

Example

IPHNIPTKI:IPTOKEN=dialogic;

6.6.17 IPHNIPTKP - IP Host NameToken Configuration

This command displays configuration related to an IP hostToken.

Note: See the individual parameter definitions of the config.txt command IP_TOKEN defined in the user manual for a full description of the parameters supported.

Syntax

IPHNIPTKP:[IPTOKEN =];

Web Management Location

System Administration > Server Management > IP Host NamesTokens > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

MMI Prerequisites

If the IP token is specified it must already have been initiated.

Example

IPHNIPTKP;

Output Format

```
IPTOKEN          IPADDR
dialogic         173.210.122.61
```

6.6.18 IPWSP - IP Web Server Configuration

This command displays the configuration for web services.

Syntax

IPWSP;

Web Management Location

System Administration > Server Management > Web Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Output Format

```
IP Web Service Configuration
WEBSERV HTTPPORT HTTPSPORT HTTPSCERT
MGMT     80       443       NONE
WSAPI    81       442       NONE
```

6.6.19 IPWSS - Configuration Web Service Set

This command configures parameters for web services. It allows HTTP and HTTPS Port numbers and the type of Certificate for HTTPS to be specified.

Syntax

IPWSS:WEBSERV=[MGMT|WSAPI],{[HTTPPORT=,][HTTPSPORT=,][HTTPSCERT=,]};

Web Management Location

System Administration > Server Management > Web Servers > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Update Access

Example

```
IPWSS:WEBSERV=MGMT,HTTPPORT=0,HTTPSPORT=443;
```

6.7 MAP Services Commands

"MAHRI / MAHRC / MAHRE - MAP HLR Rx Profile"

"MAHTI / MAHTC / MAHTE - MAP HLR Tx Profile"

"MAHTP - MAP HLR Tx Profile Print"

"MAORI / MAORC / MAORE- MAP MO-SMS Rx Profile"

"MAORP - MAP MO-SMS Rx Profile Print"

"MAOTI / MAOTC / MAOTE - MAP MO-SMS Tx Profile"

"MAOTP - MAP MO-SMS Tx Profile Print"

"MARTI / MARTC / MARTE - MAP Ready for SM Tx Profile"

"MARTP - MAP Ready for SM Tx Profile Print"

"MASPI / MASPC / MASPE - MAP Subscriber Profiling Profile"

"MASPP - MAP Subscriber Profiling Profile Print"

"MASPP - MAP Subscriber Profiling Profile Print"

"MATRI /MATRC / MATRE - MAP MT-SMS Rx Profile"

"MATRP - MAP MT-SMS Rx Profile Print"

"MATTI / MATTC / MATTE - MAP MT-SMS Tx Profile"

"MATTP - MAP MT-SMS Tx Profile Print"

"IPHNI / IPHNE - IP Host Configuration"

"IPHNP - IP Host Configuration Print"

"MAULI / MAULC / MAULE - MAP Update Location"

"MAUPI / MAUPC / MAUPE - MAP USSD Profile"

"MAUPP - MAP USSD Profile Print"

6.7.1 MAHRI / MAHRC / MAHRE - MAP HLR Rx Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Receive HLR service profiles.

Syntax

MAHRI:PROFILE=,NAME=,{[NC=,][HLRNP=,][HLRTON=,][HLRADDR=,]
[RCOPT=,][,OPTIONS=]};

MAHRC:PROFILE=,{[NAME=,][HLRNP=,][HLRTON=,][HLRADDR=,][RCOPT=,]
[,OPTIONS=]};

MAHRE:PROFILE=;

Web Management Location

System Administration > MAP Services > HLR > HLR Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The HLR address must be unique within the network context.

Examples

MAHRI:PROFILE=0,NAME=HLRADDR_RECV_0,HLRADDR=32331545;

MAHRC:PROFILE=0,HLRADDR=32331545;

MAHRE:PROFILE=0;

6.7.2 MAHRP - MAP HLR Rx Profile Print

Synopsis

Command to display the configuration associated with MAP Receive HLR service profiles.

Syntax

MAHRP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > HLR > HLR Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MAHRP:PROFILE=0;

Output Format

MAP HLR Rx Profile

PROFILE 0

NAME HLRADDR_RECV_0

NC NC0

HLRTON International

HLRNP ISDN

HLRADDR 666666666666

RCOPT N

OPTIONS 0x00000000

6.7.3 MAHTI / MAHTC / MAHTE - MAP HLR Tx Profile

Synopsis

Commands to initiate, change and end the configuration associated with MAP Transmit HLR service profiles.

Syntax

MAHTI:PROFILE=,NAME=,HLRADDR=,{[NC=,][HLRNP=,][HLRTON=,]
[RCOPT=,][,OPTIONS=][,RIID=]};

MAHTC:PROFILE=,{[NAME=,][HLRNP=,][HLRTON=,][HLRADDR=,][RCOPT=,]
[,OPTIONS=][,RIID=]};

MAHTE:PROFILE=;

Web Management Location

System Administration > MAP Services > HLR > HLR Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The HLR address must be unique within the network context.

Example

MAHTI:PROFILE=0,NAME=HLRADDR_TRANS_0,HLRADDR=32331545;

MAHTC:PROFILE=0,HLRADDR=32331545;

MAHTE:PROFILE=0;

6.7.4 MAHTP - MAP HLR Tx Profile Print

Synopsis

Command to display the configuration associated with MAP Transmit HLR service profiles.

Syntax

MAHTP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > HLR > HLR Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MAHTP:PROFILE=0;

Output Format

MAP HLR Tx Profile

PROFILE 0

NAME HLRADDR_TRANS_0

NC NC0

HLRTON International

HLRNP ISDN

HLRADDR 666666666666

RCOPT N

OPTIONS 0x00000000

RIID 0

6.7.5 MAORI / MAORC / MAORE- MAP MO-SMS Rx Profile

Synopsis

Commands to initiate, change and end the configuration associated with MAP Receive MO-SMS service profiles.

Syntax

MAORI:PROFILE=,NAME=,{[NC=,][SCTON=,][SCNP=,][SCADDR=,]
[RCOPT=,][,OPTIONS=][ASC=,] };

MAORC:PROFILE=,{[NAME=,][SCTON=,][SCNP=,][SCADDR=,][RCOPT=,]
[,OPTIONS=][ASC=,] };

MAORE:PROFILE=;

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The service center address must be unique within the network context.

Example

MAORI:PROFILE=0,NAME=MOSMS_RECV_0,SCADDR=223232222;

MAORC:PROFILE=0,SCADDR=223232222;

MAORE:PROFILE=0;

6.7.6 MAORP - MAP MO-SMS Rx Profile Print

Synopsis

Command to display the configuration associated with MAP Receive MO-SMS service profiles.

Syntax

MAORP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MAORP:PROFILE=0;

Output Format

MAP MO-SMS Rx Profile

PROFILE 0

NAME MOSMS_RECV_0

NC NC0

SCTON International

SCNP ISDN

SCADDR 666666666666

RCOPT N

OPTIONS 0x00000000

ASC MAN

6.7.7 MAOTI / MAOTC / MAOTE - MAP MO-SMS Tx Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Transmit MO-SMS service profiles.

Syntax

MAOTI:PROFILE=,NAME=,MSCADDR=,ORGADDR=,DSTSCADDR=,
{[NC=,][MSCTON=,][MSCNP=,][ORGTON=,][ORGNP=,]
[DSTSCTON=,][DSTSCNP=,][RCOPT=,][OPTIONS=][,RRID=]};

MAOTC:PROFILE=,{[NAME=,][MSCTON=,][MSCNP=,][MSCADDR=,]
[ORGTON=,][ORGNP=,][ORGADDR=,][DSTSCTON=,][DSTSCNP=,]
[DSTSCADDR=],[RCOPT=,][OPTIONS=][,RRID=]};

MAOTE:PROFILE=;

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The MSC address must be unique within the network context.

Example

```
MAOTI:PROFILE=0,NAME=MOSMS_TRANS_0,MSCADDR=123456,
      ORGADDR=24333, DSTSCADDR=2211563456;

MAOTC:PROFILE=0,MSCADDR=123456,ORGADDR=24333;

MAOTE:PROFILE=0;
```

6.7.8 MAOTP - MAP MO-SMS Tx Profile Print

Synopsis

Command to display the configuration associated with MAP Transmit MO-SMS service profiles.

Syntax

MAOTP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

```
MAOTP:PROFILE=0;
```

Output Format

```
MAP MO-SMS Tx Profile

PROFILE     0

NAME        MOSMS_TRANS_0

NC          NC0

MSCTON      International

MSCNP       ISDN

MSCADDR     666666666666

ORGTON      International

ORGNP       ISDN

ORGADDR     666666666666
```

DSTSCTON International

DSTSCNP ISDN

DSTSCADDR 666666666666

RCOPT N

OPTIONS 0x00000000

RIID 0

6.7.9 MARTI / MARTC / MARTE - MAP Ready for SM Tx Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Ready for SM service profiles.

Syntax

MARTI:PROFILE=,NAME=,SCADDR=,HLRADDR=,{[NC=,][SCTON=,][SCNP=,]
[HLRTON=,][HLRNP=,][RCOPT=,][NSUBP=,][,RIID=]} ;

MARTC:PROFILE=,{[NAME=,][SCTON=,][SCNP=,][SCADDR=,][HLRTON=,]
[HLRNP=,][HLRADDR=,][RCOPT=,][NSUBP=,][,RIID=]} ;

MARTE:PROFILE=;

Web Management Location

System Administration > MAP Services > SMS > Ready for SM > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The service center address must be unique within the network context.

Example

MARTI:PROFILE=0,NAME=READYSM_TRANS_0,SCADDR=23323121,HLRADDR=1121212;

MARTC:PROFILE=0,HLRADDR=1121212;

MARTE:PROFILE=0;

6.7.10 MARTP - MAP Ready for SM Tx Profile Print

Synopsis

Command to display configurations associated with MAP Ready for SM service profiles.

Syntax

MARTP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > Ready for SM > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MARTP:PROFILE=0;

Output Format

MAP Ready for SM service profile

PROFILE 0

NAME READYSM_TRANS_0

NC NC0

SCTON International

SCNP ISDN

SCADDR 666666666666

HLRTON International

HLRNP ISDN

HLRADDR 666666666666

RCOPT N

NSUBP N

RIID 0

6.7.11 MASPI / MASPC / MASPE - MAP Subscriber Profiling Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Subscriber service profiles.

Syntax

MASPI:PROFILE=,NAME=,GWADDR=,{[NC=,][GWNP=,][GWTON=,]
[DSTTON=,][DSTNP=,][RCOPT=,][,OPTIONS=][,RIID=]};

MASPC:PROFILE=,{[NAME=,][GWNP=,][GWTON=,][GWADDR=,]
[DSTTON=,][DSTNP=,][RCOPT=,][,OPTIONS=][,RIID=,]};

MASPE:PROFILE=;

Web Management Location

System Administration > MAP Services > Subscriber > Subscriber > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The gateway address must be unique within the network context.

Example

MASPI:PROFILE=0,NAME=SUBPROF_TRANS_0,GWADDR=33233232;

MASPC:PROFILE=0,GWADDR=33233232;

MASPE:PROFILE=0;

6.7.12 MASPP - MAP Subscriber Profiling Profile Print

Synopsis

Command to display configurations associated with MAP Subscriber service profiles.

Syntax

MASPP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > Subscriber > Subscriber > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MASPP:PROFILE=0;

Output Format

MAP Subscriber service profile

PROFILE 0

NAME SUBPROF_TRANS_0

NC NC0

GWTON International

GWNP ISDN

GWADDR 666666666666

DSTTON International

DSTNP ISDN

RCOPT N

OPTIONS 0x00000000

RIID 0

6.7.13 MATRI /MATRC / MATRE - MAP MT-SMS Rx Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Receive MT-SMS service profiles.

Syntaxf

MATRI:PROFILE=,NAME=,{[NC=,][SCTON=,][SCNP=,][SCADDR=,]
[RCOPT=,][TXTPREF=,][,OPTIONS=]};

MATRC:PROFILE=,{NAME=,][SCTON=,][SCNP=,][SCADDR=,][RCOPT=,]
[TXTPREF=,][,OPTIONS=]};

MATRE:PROFILE=;

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The service center address must be unique within the network context.

The profile cannot be ended if it is still associated with MAP Update Location configuration.

Example

MATRI:PROFILE=0,NAME=MTSMS_RECV_0,SCADDR=123456789;

MATRC:PROFILE=0,SCADDR=123456789;

MATRE:PROFILE=0;

6.7.14 MATRP - MAP MT-SMS Rx Profile Print

Synopsis

Command to display the system configurations associated with MAP Receive MT-SMS service profiles.

Syntax

MATRP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Rx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MATRP:PROFILE=0;

Output Format

MAP MT-SMS Rx Profile

PROFILE 0

NAME MTSMS_RECV_0

NC NC0

SCTON International

SCNP ISDN

SCADDR 666666666666

TXTPREF Y

RCOPT N

OPTIONS 0x00000000

6.7.15 MATTI / MATTC / MATTE - MAP MT-SMS Tx Profile

Synopsis

Commands to initiate, change and end configurations associated with MAP Transmit MT-SMS service profiles.

Syntax

MATTI:PROFILE=,NAME=,SCADDR=,ORGADDR=,{[NC=,][SCTON=,]
[SCNP=,][ORGTON=,][ORGNP=,][DSTTON=,][DSTNP=,]
[RCOPT=,][RDEL=,][,HLRRIID=][,MSCRIID=]};

MATTC:PROFILE=,{NAME=,][SCTON=,][SCNP=,][SCADDR=,][ORGTON=,]
[ORGNP=,][ORGADDR=,][DSTTON=,][DSTNP=,][RCOPT=,]
[RDEL=,][,HLRRID=][,MSCRIID=]};

MATTE:PROFILE=;

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The service center address must be unique within the network context.

Example

MATTI: PROFILE=0,NAME=TR0,SCADDR=1234567,ORGADDR=7654321;

MATTC: PROFILE=0,RCOPT=Y;

MATTE:PROFILE=0;

6.7.16 MATTP - MAP MT-SMS Tx Profile Print

Synopsis

Command to display configurations associated with MAP Transmit MT-SMS service profiles.

Syntax

MATTP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Tx > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MATTP:PROFILE=0;

Output Format

MAP MT-SMS Tx Profile

PROFILE 0

NAME MTSMS_TRANS_0

NC NC0

SCTON International

SCNP ISDN

SCADDR 666666666666

ORGTON International

ORGNP ISDN

ORGADDR 666666666666

DSTTON International

DSTNP ISDN

RCOPT N

OPTIONS 0x00000000

RDEL N

HLRRIID 0

MSCRIID 0

6.7.17 MAULI / MAULC / MAULE - MAP Update Location

Synopsis

Commands to initiate and change configurations associated with MAP Update Location Web Services.

Syntax

MAULI:IMSI=,HLRTON=,HLRNP=,HLRADDR=,PROFILE=

MAULC:IMSI=,[HLRTON=,][HLRNP=,][HLRADDR=,][PROFILE=,]

MAULE:IMSI=;

Web Management Location

System Administration > MAP Services > Update Location > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile is an initiated MT-SMS Rx profile.

Example

MAULI:IMSI=1212122,HLRTON=International,HLRNP=ISDN,HLRADDR=332334423,PROFILE=0;

MAULC:IMSI=1212122,HLRTON=International;

MAULE:IMSI=1212122;

MAULP - MAP Update Location Configuration

Synopsis

This command displays the system configuration associated with MAP Update Location Web Services.

Synopsis

MAULP;

Web Management Location

System Administration > MAP Services > Update Location > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MAULP;

Output Format

MAP Update Location Services

```
IMSI        HLRTON           HLRNP    HLRADDR       PROFILE
1212122      International      ISDN     332334423      0
```

6.7.18 IPHNI / IPHNE - IP Host Configuration

Commands to dynamically initiate and end configuration related to an IP Host.

To dynamically add configuration, first add a new IP_HOST command in the config.txt file and then execute the IPHNI command to load the configuration into the system.

To dynamically remove configuration, first remove the IP_HOST command from the config.txt file and then execute the IPHNE command to remove the configuration from the system.

Syntax

IPHNI:IPHOST_NAME=;

IPHNE:IPHOST_NAME=;

Web Management Location

System Administration > Server Management > IP Host > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Update Access

Prerequisites

There are no startup parse or configuration errors present in the alarm log.

Example

IPHNI:IPHOST_NAME=dsh-0015b2a48c04;

IPHNE:IPHOST_NAME=dsh-0015b2a48c04;

6.7.19 IPHNP - IP Host Configuration Print

This command displays configuration related to an IP Token as configured by the IP_HOST command in config.txt.

Syntax

IPHNP:[IPHOST_NAME=];

Web Management Location

System Administration > Server Management > IP Host > Configuration

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Prerequisites

If the IP Hostname is specified it must already have been initiated.

Example

IPHNP;

Output Format

```
IP Host Configuration
IPHOST_NAME                IPTOKEN
dsh-0015b2a48c04c          Austin
```

6.7.20 MAUPI / MAUPC / MAUPE - MAP USSD Profile

Commands to initiate, change and end configurations associated with MAP USSD service profiles.

Syntax

```
MAUPI:PROFILE=,NAME=,GWADDR=,{[NC=,][GWTON=,][GWNP=,]
        [DSTTON=,][DSTNP=,][DFDCS=,][LANG=,][RCOPT=,]
        [,OPTIONS=][RCV_GWTON=,][RCV_GWNP=,][RCV_GWADDR=,]};

MAUPC:PROFILE=,{[NAME=,][GWTON=,][GWNP=,][GWADDR=,][DSTTON=,]
         [DSTNP=,][DFDCS=,][LANG=,][RCOPT=,][,OPTIONS=]
         [RCV_GWTON=,][RCV_GWNP=,][RCV_GWADDR=,]};

MAUPE:PROFILE=;
```

Web Management Location

System Administration > MAP Services > USSD > USSD > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Update Access

Prerequisites

The profile and name must be unique for the service.

The gateway address must be unique within the network context.

Example

```
MAUPI:PROFILE=0,NAME=USSD_0,GWADDR=1212321234;

MAUPC:PROFILE=0,GWADDR=1212321234;

MAUPE:PROFILE=0;
```

6.7.21 MAUPP - MAP USSD Profile Print

Command to display configurations associated with MAP USSD service profiles.

Syntax

MAUPP:[PROFILE=,];

Web Management Location

System Administration > MAP Services > USSD > USSD > Configuration

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MAUPP:PROFILE=0;

Output Format

MAP USSD service profile

PROFILE 0

NAME USSD_0

NC NC0

GWTON International

GWNP ISDN

GWADDR 666666666666

RCV_GWTON International

RCV_GWNP ISDN

RCV_GWADDR ANY

DSTTON International

DSTNP ISDN

DEFDSC English

LANG EN

RCOPT N

OPTIONS 0x00000000
RIID 0

6.8 MMI Commands

"MMLOI - MMI Logoff Initiate"

"Maintenance Commands"

"Maintenance Commands"

6.8.1 MMLOI - MMI Logoff Initiate

This command ends the current log-on session.

Syntax

MMLOI;

Web Management Location

Command line only

Applicability

Operating Modes: SIU, SWS, DSH

Example

MMLOI;

6.9 Maintenance Commands

"MNINE - Maintenance Uninhibit Initiate"

"MNINI - Maintenance Inhibit Initiate"

"MNRSI - Maintenance Restart Initiate"

"MNSSI - Maintenance Snapshot Initiate"

6.9.1 MNINE - Maintenance Uninhibit Initiate

This command activates an SS7 signaling link, SIGTRAN M3UA link, host RSI link or circuit group. The command is also used to uninhibit an SS7 signaling link and to unblock a newly installed hard disk drive following hard disk drive failure.

Important: In order to maintain RAID array hard disk drive integrity, it is important follow the correct procedure as detailed in the operators manual when unblocking hard disk drives.

Syntax

MNINE:[LINK=[,INHIBIT=N]]|[HOSTID=]|[GID=]|[SNLINK=]|[DRIVE=];

Web Management Location

LINK - System Administration > SS7 > SS7 Links > Status

HOSTID - System Administration > Hosts > Hosts > Status

GID - System Administration > Call > Circuit Groups > Status

SNLINK - System Administration > SIGTRAN > Links > Status

DRIVE - System Administration > Server Management > Disk Drives > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

If activating a link the SS7 signaling link set has not already been activated

If uninhibiting a link the link has been activated.

The circuit group must be already configured and deactivated.

Only M3UA SIGTRAN links may be activated.

The disk drive must be in the INACTIVE state.

Example

MNINE:LINK=3; MNINE:LINK=3,INHIBIT=N; MNINE:HOSTID=1; MNINE:GID=2; MNINE:DRIVE=1;

6.9.2 MNINI - Maintenance Inhibit Initiate

This command is deactivates an SS7 signaling link, SIGTRAN M3UA link, host RSI link or circuit group. The command is also used to inhibit an SS7 signaling link and to block a failed hard disk drive before removal and replacing.

Important: In order to maintain RAID array hard disk drive integrity it is important to follow the correct procedure as detailed in the operators manual when blocking hard disk drives.

> ***Note:*** To inhibit a signaling link, the command should be entered with the INHIBIT=Y parameter set. The SS7 Link status MMI command should then be used to determine the (new) status of the link. If the inhibit request was accepted the L3 STATE is shown as UNAVAILABLE. However, if the inhibit request was denied (for example because it relates to the only active link), the L3 STATE is shown as AVAILABLE.

Syntax

MNINI: [LINK=[,INHIBIT=Y]]|[HOSTID=]|[GID=]|[SNLINK=]|[DRIVE=];

Web Management Location

LINK - System Administration > SS7 > SS7 Links > Status

HOSTID - System Administration > Hosts > Hosts > Status

GID - System Administration > Call > Circuit Groups > Status

SNLINK - System Administration > SIGTRAN > Links > Status

DRIVE - System Administration > Server Management > Disk Drives > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

If the link is to be inhibited it must be active.

The last link in a SS7 signaling linkset cannot be inhibited.

The circuit group must be already configured and activated.

Only M3UA SIGTRAN links may be deactivated.

The Disk drive must be active and not in the RESTARTING state.

Example

MNINI:LINK=4; MNINI:LINK=4,INHIBIT=Y; MNINI:HOSTID=1; MNINI:GID=4; MNINI:DRIVE=1;

6.9.3 MNPCS - Maintenance PCM Control Set

This command allows specific conditions to be applied to an E1/T1 PCM interface for diagnostic purposes. Typically this command is used during type testing of the E1/T1 interface.

This command allows the user to control the generation of AIS (Blue alarm), to activate various diagnostic loopback modes, and to activate generation of PRBS test sequences.

If the system is restarted, any active control actions will be discarded.

Syntax

MNPCS:PORTID=[,AISGEN=][,LOOPMD=][,PRBSGEN=];

Web Management Location

This diagnostic command is not available on the browser interface.

Applicability

Operating Modes: ALL

Permissions: System Maintenance Access

Prerequisites

he action must be supported by the particular board type.

Example

MNPCS:PORTID=4,AISGEN=2;

MNPCS:PORTID=4,LOOPMD=3;

MNPCS:PORTID=4,PRBSGEN=3;

6.9.4 MNRSI - Maintenance Restart Initiate

This command will restart the entire system. The current log-on session will be terminated.

If system type is set, the system type will change after restart.

> ***Note:*** To install a new mode software license or software distribution for the first time the software or license must be loaded onto the system and system re-booted before the new mode can be entered.

If RESET=Y, all configuration and log files in the syslog directory will be removed during restart. If not resetting after restart no change to the system configuration will occur and the state of all links will automatically be restored.

If DEFBMC=Y, Configuration related to Lights Out Management will be reset to its default values. This include the IP Address and login password for Lights Out Management. Only users with System Administration Access can set this parameter.

Syntax

MNRSI:[SYSTYPE=,RESTART=][RESET=Y,][DEFBMC=Y,];

Web Management Location

System Administration > Software > System Software > Configuration Operations > Restart

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

Only system types that have been licensed can be specified.

Only system types where the supporting software is present on the unit. Can be selected.

Example

MNRSI;

6.9.5 MNSSI - Maintenance Snapshot Initiate

This command will take a new snapshot of the system diagnostic logs.

This command takes a snapshot of key system data. Once executed, all snapshot data (excluding binary files) will be written to a single file (snapshot.tgz) in the root directory of the ftpuser account. If TRACE is set to Y, then snapshot.tgz will include trace log files. If the parameter is not set or set to N, then trace log files will be excluded from the snapshot.

Syntax

MNSSI:[TRACE=Y];

Web Management Location

Operations > Snapshot

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Example

MNSSI;

6.10 Message Router Commands

"MRCEE - Message Router Concerned Entity End"

"MRCEI - Message Router Concerned Entity Initiate"

"MRCEP - Message Router Concerned Entity Configuration"

"MRCPE - Message Router Custom Profile End"

"MRCPI - Message Router Custom Profile Initiate"

"MRCPP - Message Router Custom Profile Configuration"

"MRDEE - Message Router Destination End"

"MRDEI - Message Router Destination Initiate"

"MRDEP - Message Router Destination Configuration"

"MROGE-Message Router Origin Configuration"

"MROGI - Message Router Origin Configuration"

"MROGP - Message Router Origin Configuration"

"MRRKI - Message Router Routing Key Initiate"

"MRRKE - Message Router Routing Key End"

"MRRKI - Message Router Routing Key Initiate"

"MRRKP - Message Router Routing Key Configuration"

6.10.1 MRCEE - Message Router Concerned Entity End

The command removes a new Concerned Entity.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command MRF_CE entry from the config.txt file.
2) Executing the MRCEE MMI command to unload it from the system.

Syntax

MRCEE:CONCID=;

Web Management Location

System Administration > Message Router > Concerned Entity > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Concerned Entity has been initiated.
The Concerned Entity is not present in the config.txt file.
The Concerned Entity is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The Concerned Entity is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

MRCEE:CONCID=1;

6.10.2 MRCEI - Message Router Concerned Entity Initiate

This command adds a new Concerned Entity.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, MRF_CE, in the config.txt file.
2) Executing the MRCEI MMI command to load that configuration.

Syntax

MRCEI:CONCID=;

Web Management Location

System Administration > Message Router > Concerned Entity > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Concerned Entity has not been initiated.
A value of ANY cannot be used for a DPC when dynamically adding a new Concerned Entity.
The Concerned Entity is present in the config.txt file.
There are no startup parse or configuration errors present.
The Concerned Entity is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

MRCEI:CP=1;

6.10.3 MRCEP - Message Router Concerned Entity Configuration

This command displays all configured Message Router Concerned Entitys.

Note: See the individual parameter definitions of the config.txt command MRF_CE defined in the user manual for a full description of the parameters supported.

Syntax

MRCEP:[CONCID=];

Web Management Location

System Administration > Message Router > Concerned Entity > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MRCEP;

Output Format

```
Message Router Concerned Entity Configuration
CONCID NC  DPC       CONC_DOMAIN CONC_NC CONC_ENT  ALIAS
0      NC0 44343434  NETWORK     NC0     2332
1      NC0 123233    AS          NC0     ANY
```

6.10.4 MRCPE - Message Router Custom Profile End

The command removes a new Custom Profile.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command MRF_CP entry from the config.txt file.
2) Executing the MRCPE MMI command to unload it from the system.

Syntax

MRCPE:CP=;

Web Management Location

System Administration > Message Router > Custom Profile > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Custom Profile has been initiated.
The Custom Profile is not present in the config.txt file.
The Custom Profile is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The Custom Profile is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

MRCPE:CP=1;

6.10.5 MRCPI - Message Router Custom Profile Initiate

This command adds a new Custom Profile.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, MRF_CP, in the config.txt file.
2) Executing the MRCPI MMI command to load that configuration.

Syntax

MRCPI:CP=;

Web Management Location

System Administration > Message Router > Custom Profile > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Custom Profile has not been initiated.
The Custom Profile is present in the config.txt file.
There are no startup parse or configuration errors present.
The Custom Profile is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

MRCPI:CP=1;

6.10.6 MRCPP - Message Router Custom Profile Configuration

This command displays all configured Message Router Custom Profiles.

Note: See the individual parameter definitions of the config.txt command MRF_CP defined in the user manual for a full description of the parameters supported.

Syntax

MRCPP:[CP=];

Web Management Location

System Administration > Message Router > Custom Profile > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MRCPP;

Output Format

```
Message Router Custom Profile Configuration
CP    OPC       DPC       NI        SI          LABEL
0     NONE     2332      0        NONE
1     123233    NONE      NONE      NONE
```

6.10.7 MRDEE - Message Router Destination End

The command removes a new Destination.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command MRF_DE entry from the config.txt file.
2) Executing the MRDEE MMI command to unload it from the system.

Syntax

MRDEE:DESTID=;

Web Management Location

System Administration > Message Router > Destination > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Destination has been initiated.
The Destination is not present in the config.txt file.
The Destination is not used in any other configuration.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The Destination is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

MRDEE:DESTID=1;

6.10.8 MRDEI - Message Router Destination Initiate

This command adds a new Destination.

Note: Traffic routed to a partner System with a destination DOMAIN of "PARTNER" will be consider on the receiving system to be either from the original "NETWORK", "AS" or "USER" domains of the transmitting System.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, MRF_DE, in the config.txt file.
2) Executing the MRDEI MMI command to load that configuration.

Syntax

MRDEI:DESTID=;

Web Management Location

System Administration > Message Router > Destination > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Destination has not been initiated.
The Destination is present in the config.txt file.
There are no startup parse or configuration errors present.
The Destination is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

MRDEI:DESTID=1;

6.10.9 MRDEP - Message Router Destination Configuration

This command displays all configured Message Router Destinations.

Note: See the individual parameter definitions of the config.txt command MRF_DE defined in the user manual for a full description of the parameters supported.

Syntax

MRDEP:[DESTID=];

Web Management Location

System Administration > Message Router > Destination > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MRDEP;

Output Format

```
 Message Router Destination Configuration
  DESTID DEST    DESTSEQ NC   DOMAIN  RAS   DPC   CP    LABEL
  0      1       1       NC0  AS      1     NONE
  1      2       1       NC0  NETWORK       NONE  NONE  1
```

6.10.10 MROGE-Message Router Origin Configuration

Command to dynamically remove an Origin.

To dynamically remove an Origin, first remove the MRF_OG command from the config.txt file and then execute the MROGE command to remove the configuration from the system.

Syntax

MROGE:OGID=;

Web Management Location

System Administration > Message Router > Origin > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

Prerequisites

The Origin has been initiated.

The Origin is not present in the config.txt file.

There are no startup parse or configuration errors present in the alarm log.

In order to dynamically remove an Origin there must be at least one other active Origin using the same NC/DOMAIN/SI combination.

Example
MROGE:OGID=1;

6.10.11 MROGI - Message Router Origin Configuration

Command to dynamically add a new Message Router Origin.

To dynamically add a new Origin, first add a new MRF_OG command in the config.txt file and then execute the MROGI command to load the configuration into the system.

Syntax

MROGI:OGID=;

Web Management Location

System Administration > Message Router > Origin > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

Prerequisites

There are no startup parse or configuration errors present in the alarm log.

The Origin is present in the config.txt file.

In order to dynamically add an Origin, there must already be at least one active Origin using the same NC/DOMAIN/SI combination.

Domain must be set to one of these: NETWORK, AS or UPART.

Example
MROGI:OGID=1;

6.10.12 MROGP - Message Router Origin Configuration

This command displays all configured Message Router Origins.

Note: See the individual parameter definitions of the config.txt command MRF_OG defined in the user manual for a full description of the parameters supported.

Syntax

MROGP:[OGID=];

Web Management Location

System Administration > Message Router > Origin > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MROGP;

Output Format

```
Message Router Origin Configuration
OGID NC  DOMAIN SI          OPC       RKTAB CP    LABEL
0    NC0 M3UA   3           ANY       1     NONE
1    NC0 MTP    3           ANY       1     1
```

6.10.13 MRRKI - Message Router Routing Key Initiate

This command adds a new Routing Key.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, MRF_RK, in the config.txt file.
2) Executing the MRRKI MMI command to load that configuration.

Syntax

MRRKI:RKI=;

Web Management Location

System Administration > Message Router > Routing Key > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Routing Key has not been initiated.
The Routing Key is present in the config.txt file.
There are no startup parse or configuration errors present.
The Routing Key is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

MRRKI:RKI=1;

6.10.14 MRRKE - Message Router Routing Key End

The command removes a new Routing Key.

Note: Configuration may be dynamically removed by:

1) Deleting a configuration command MRF_RK entry from the config.txt file.
2) Executing the MRRKE MMI command to unload it from the system.

Syntax

MRRKE:RKI=;

Web Management Location

System Administration > Message Router > Routing Key > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Routing Key has been initiated.
The Routing Key is not present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.
There are no startup parse or configuration errors present.
The Routing Key is present in the config.txt file.

Note: Circuit Groups are dynamically removed by first deleting the group from the config.txt file.

Example

MRRKE:RKI=1;

6.10.15 MRRKI - Message Router Routing Key Initiate

This command adds a new Routing Key.

Note: Configuration may be dynamically added by:

1) Entering an additional configuration command, MRF_RK, in the config.txt file.
2) Executing the MRRKI MMI command to load that configuration.

Syntax

MRRKI:RKI=;

Web Management Location

System Administration > Message Router > Routing Key > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Update Access

MMI Prerequisites

The Routing Key has not been initiated.
The Routing Key is present in the config.txt file.
There are no startup parse or configuration errors present.
The Routing Key is present in the config.txt file.
There are no restart or configuration failed alarms present in the alarm log.

Example

MRRKI:RKI=1;

6.10.16 MRRKP - Message Router Routing Key Configuration

This command displays all configured Message Router Routing Keys.

Note: See the individual parameter definitions of the config.txt command MRF_RK defined in the user manual for a full description of the parameters supported.

Syntax

MRRKP:[RKI=];

Web Management Location

System Administration > Message Router > Routing Key > Configuration

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MRRKP;

Output Format

```
Message Router Routing Keye Configuration
RKI   RKTAB OPC        DPC         NI    SI   CIC_RANGE  HUNT      DEST  LABEL
0     1     2          123233      ANY   ANY  ANY        FIRST     5
1     1     123233     2           ANY   ANY  ANY        FIRST     6
```

6.11 Measurement Commands

“MSACP - ATM Cell Stream Traffic Measurements”

“MSCGP - Circuit Group Measurements”

“MSCRP - SS7 Route Measurements”

“MSDBP – Subscriber Database Service Measurements”

“MSDEP - Message Router Destination Measurements”

“MSDHP - DTS Host Measurements”

“MSFEP - Flow Environment Measurements”

“MSHPP - Diameter Peer Measurements”

“MSHLP - Host Link Measurements”

“MSLCP - Software License Capability Measurements”

“MSHLP - Host Link Measurements”

“MSLCP - Software License Capability Measurements”

“MSLTP - SCCP Loadshare Table Measurements”

“MSMLP - SS7 Monitor Link Measurements”

“MSNIP - Network Interface Measurements”

“MSOGP - Message Router Origin Measurements”

“MSPCP - PCM Measurements”

“MSRAP - SIGTRAN Remote Application Server Measurements”

“MSRKP - Message Router Routing Key Measurements”

“MSRLP - Remote Server Link Measurements”

“MSSLP - SS7 Link Measurements”

“MSSRP - SIGTRAN Route Measurements”

“MSSRP - SIGTRAN Route Measurements”

“MSSTP - SIGTRAN Link Measurements”

“MSSYP - System Measurements”

“MSHRP - MAP HLR Rx Measurements”

“MSHTP - MAP HLR Tx Measurements”

“MSORP - MAP MO-SMS Rx Measurements”

“MSOTP - MAP MO-SMS Tx Measurements”

“MSRTP - MAP Ready for SM Tx Profile Measurements”

“MSSPP - MAP Subscriber Profiling Measurements”

“MSTRP - MAP MT-SMS Rx Measurements”

“MSTTP - MAP MT-SMS Tx Measurements”

“MSUPP - MAP USSD Measurements”

"MSHRP - MAP HLR Rx Measurements"

"MSHTP - MAP HLR Tx Measurements"

"MSORP - MAP MO-SMS Rx Measurements"

"MSOTP - MAP MO-SMS Tx Measurements"

"MSRTP - MAP Ready for SM Tx Profile Measurements"

"MSSPP - MAP Subscriber Profiling Measurements"

"MSTRP - MAP MT-SMS Rx Measurements"

"MSTTP - MAP MT-SMS Tx Measurements"

"MSUPP - MAP USSD Measurements"

6.11.1 MSACP - ATM Cell Stream Traffic Measurements

This command displays traffic measurements for ATM Cell Streams.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSACP:[RESET=,];

Web Management Location

System Administration > Boards > Cell Streams > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSACP; MSACP:RESET=Y;

Output Format

```
ATM Cell Stream Traffic Measurements
CELLSTR RXFRAME RXOCT  RXDISC RXERR  TXFRAME TXOCT  TXDISC TXERR  PERIOD
1           700 15430       0     0      721 14322       1     0  01:00:00
2            10    80       0     0       11    90       0     0  01:00:00
3           356  8220       0     0      321  7211       0     0  01:00:00
```

The meaning of each field in the output is as follows:

CELLSTR - ATM Cell Stream ID as configured in config.txt file

RXFRAME – Number of valid AAL5 frames received.

RXOCT – Number of data octets received.

RXDISC – Number of received AAL5 frames discarded.

RXERR - Number of frames with errors received.

TXFRAME – Number of valid AAL5 frames.

TXOCT – Number of data octets transmitted.

TXDISC – Number of transmitted AAL5 frames discarded.

TXERR - Number of frames with errors transmitted.

PERIOD - Time since measurements on the port were last reset.

6.11.2 MSCGP - Circuit Group Measurements

This command displays measurements for the configured circuit groups.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSCGP:[RESET=];

Web Management Location

System Administration > Call > Circuit Groups > Stats

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

MSCGP; MSCGP:RESET=Y;

Output Format

```
Circuit group status
CGRP IOFF   IANS   OGOFF  OGANS  MAXDEV ACCUM  PERIOD
0    5      5      0      0      30      0      00:00:30
1    332    5      65665  0      30      0      00:00:30
```

The meaning of each field in the output is as follows:

GID - Circuit Group ID.

IOFF - The number of incoming calls attempted.

IANS - The number of incoming calls answered.

OGOFF - The number of outgoing calls attempted.

OGANS - The number of outgoing calls answered.

MAXDEV - Maximum number of devices active in the group at any time.

ACCUM - The accumulated call duration.

PERIOD - The measurement period.

6.11.3 MSCRP - SS7 Route Measurements

This command displays traffic measurements for SS7 routes.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSCRP:[RESET =,];

Web Management Location

System Administration > SS7 > SS7 Routes > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSCRP; MSCRP:RESET=Y;

Output Format

```
SS7 Route Measurements
C7RT OOSDUR NOOS RXMSU RXOCT TXMSU TXOCT  PERIOD
0    0      0    375   8220  16320 124306 00:12:00
1    0      0    392   8624  17036 141860 00:12:00
```

The meaning of each field in the output is as follows:

C7RT - SS7 route.

OOSDUR - Duration that the route was not in service. This field is not currently supported.

NOOS - Number of times the route went out of service.

RXMSU - Number of message signaling units octets received.

RXOCT - Number of signaling Information Field (SIF) and Service.

Information Octet (SIO) octets received.

TXMSU - Number of message signaling units octets transmitted.

TXOCT - Number of SIF and SIO octets transmitted.

PERIOD - The measurement period.

6.11.4 MSDBP – Subscriber Database Service Measurements

This command displays measurements associated with Subscriber Database Services.

Syntax

MSDBP:[RESET=Y];

Web Management Location

System Administration > Subscriber Database > Services > Stats

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

MSDBP;

Output Format

Subscriber Database Service Measurements

DBSVCID DBSVCTYPE NSERV CURSERV PEAKSERV NS5M NS1H NS1D NCONG NFAIL COUNT1 COUNT2 PERIOD

0 MNP 0 2 150 5 7 150 1 5 4000 200 00:12:00

The meaning of each field in the output is as follows:

DBSVCID – the Service ID.

DBSVCTYPE – the Service Type.

NSERV – total number of service requests.

CURSERV – current number of active service requests.

PEAKSERV – peak number of active service requests.

NS5M – peak rate of service requests during the last 5 minutes (requests/second).

NS1H – peak rate of service requests during the last hour (requests/second).

NS1D – peak rate of service requests during the last day (requests/second).

NCONG- number of congestion events.

NFAIL- number of failed service requests.

COUNT1- service specific counter 1. For MNP, the number of requests that returned a ported number.

COUNT2- service specific 2. For MNP, the number of badly formatted service requests received.

PERIOD – the period over which the measurements were taken.

6.11.5 MSDEP - Message Router Destination Measurements

This command displays traffic measurements for Message Router Routing Keys.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSDEP:[DESTID=,][[RESET=];

Web Management Location

System Administration > Message Router > Destination > Stats

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MSDEP:DESTID=4;

Output Format

```
Message Router Destination Measurements
DESTID DEST   DESTSEQ    TXMSU   TXOCT   PERIOD
4      1      2          2540    23323   01:17:45
```

The meaning of each field in the output is as follows:

DESTID - The Destination Index.
DEST - The Destination Table ID.
DESTDEQ - The row identifier within the destination table.
TXMSU - Messages transmitted to the destination for this row entry.
TXOCT - Number of octets in Messages transmitted to the destination.
PERIOD - Measurement collection period.

6.11.6 MSDHP - DTS Host Measurements

A new MMI command provides measurements on a per DTS host basis. It is defined as follows:

Synopsis

This command displays measurements for configured DTS Hosts. The user can optionally reset the measurements.

Syntax

MSDHP:[RESET=];

Web Management Location

System Administration > Transaction > DTS Hosts > Stats

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

MSDHP;
MSDHP:RESET=Y;

Output Format

```
DTS Host Measurements
HOSTID RXMSG  TXMSG  RXDISCARD TXDISCARD IDLG   ODLG   IBILL  PERIOD
0      5      5      0         0         0      0      30     00:00:30
1      332    5      65665     0         0      545    45     00:00:30
```

The meaning of each field in the output is as follows:

HOSTID - DTS Host ID.

RXMSG - Number of messages received from the network sent to the host.

TXMSG - Number of outgoing data messages from the host transmitted to the network.

RXDISCARD - Number of messages received from the network that were destined for this host but discarded.

TXDISCARD - Number of outgoing data messages from the host that were discarded.

IDLG - Number of incoming dialogues started for this host.

ODLG - Number of outgoing dialogues started from this host.

IBILL - Number of incoming dialogue started for this host using Billing ID based routing.

PERIOD - The measurement period in hours, minutes and seconds.

6.11.7 MSFEP - Flow Environment Measurements

This command displays traffic measurements for the flow environment.

Syntax

MSFEP;

Web Management Location

System Administration > Diagnostics > Flow Environment > Stats

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

MSFEP;

Output Format

```
Flow Environment Measurements
TTOTAL        0
TRANS         0
TFAIL         0
TPFAIL        0
TDROP         0
```

```
TSHUT          0
TNOFLOW        0
TTOUT          0
TCONGC         0
PERIOD         27:23:32
```

6.11.8 MSHLP - Host Link Measurements

This command displays traffic measurements for links to Application Hosts.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSHLP:[RESET =,];

Web Management Location

System Administration > Hosts > Hosts > Stats

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

MSHLP; MSHLP:RESET=Y;

Output Format

```
  Host SIU Link Measurements
  HOSTID RXMSG  TXMSG  RXOCT  TXOCT  OOSDUR NOOS   NDISCARD PERIOD
      1 1.43E6 1.45E6 5.48E6 5.35E6     62    1          0 00:14:55
      2 1.64E6 1.65E6 8.21E6 8.12E6     99    1          0 00:14:55
```

The meaning of each field in the output is as follows:

RXMSG- number of messages received.

TXMSG - number of messages transmitted.

RXOCT - number of octets received in messages excluding message header octets (rounded down to the nearest 1000).

TXOCT - number of octets transmitted in messages excluding message header octets (rounded down to the nearest 1000).

OOSDUR - the total amount time the link was out of service (in multiples of 100ms).

OOSDUR - the total amount time the link was out of service (in multiples of 100ms).

NOOS - the number of times the link went out of service.

NDISCARD - the number of messages due to be transmitted that were discarded.

PERIOD - the time period over which these statistics have been gathered (in hours, minutes and seconds).

6.11.9 MSHPP - Diameter Peer Measurements

This command displays traffic measurements for Diameter Peers.

Syntax

MSHPP:[HDPR=];

Web Management Location

System Administration > Diameter > Peer > Stats

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

MSHPP;

MSHPP:HDPR=0;

Output Format

```
Diameter Peer Measurements
HDPR    RXMSG    TXMSG    PERIOD
4       4343     4000     01:17:45
```

6.11.10 MSLCP - Software License Capability Measurements

This command shows measurements related to software licenses on the system.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSLCP:[RESET=,];

Web Management Location

System Administration > Software > Software Licenses > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSLCP;

Output Format

```
  Software License Capability Measurements
  CAPABILITY NC  RXDATA TXDATA RXPEAK TXPEAK PEAK   CONG   ENFORCE PERIOD
  M3UA       NC0   4204E5 3212E4 154    456     923      1         1 01:33:33
```

The meaning of each field in the output is as follows:

CAPABILITY – A Licensable capability of the system. This is a protocol or operating mode capability which has been purchased or is under evaluation. NC - A Network Context the capability is associated. Blank if not applicable.

RXDATA - The amount of data received in Kbytes.

TXDATA - The amount of data transmitted in Kbytes.

RXPEAK - The peak received data rate in Kbytes/s averaged over a rolling thirty second time window.

TXPEAK - The peak transmitted data rate in Kbytes/s averaged over a rolling thirty second time window.

PEAK - The peak data rate for both transmitted and received data in Kbytes/s averaged over a rolling thirty second time window.

CONGESTION - The number of times the license has exceeded its throughput threshold.

ENFORCE - The number of times the unit has enforced the license throughput limit.

PERIOD - Time since measurements on the route were last reset. Specified in hours, minutes and seconds.

6.11.11 MSLTP - SCCP Loadshare Table Measurements

This command displays traffic measurements for SCCP Loadshare Tables.

Page 1 displays summary measurements associated with each SCCP Loadshare Table.

Page 2 displays measurements for DPC associcated with a SCCP Loadshare Table.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSLTP:[RESET=,][PAGE=];

Web Management Location

System Administration > SCCP > Load Share Tables > Configuration

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSLTP;
MSLTP:PAGE=2;
MSLTP:RESET=Y;

Output Format

```
SCCP Loadshare Table Services Measurements (Page 1 of 2
LST       SUCCESS FAIL   PERIOD
LST-5     1212    2      01:29:16
LST-7     333     5      01:29:16

SCCP Loadshare Table Services Measurements (Page 2 of 2)
LSTSEQ       DPC         TXMSG  PERIOD
LST-5-0      2222        606    01:29:16
LST-5-1      2223        606    01:29:16
LST-7-0      1011        333    01:29:16
LST-7-1      1013        0      01:29:16
```

The meaning of each field in the output is as follows:

LST - The Loadshare Table identifier.
SUCCESS - Count of successful routing attempts.
FAIL - Count of failed routing attempts.
SEQ - A sequence number for a DPC in Loadshare Table.
DPC - A Destination Point Code.
TXMSG - The number of messages routed to the DPC.
PERIOD - Time since measurements for the service were last reset.

6.11.12 MSMLP - SS7 Monitor Link Measurements

This command displays traffic measurements for Monitor links.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSMLP:[RESET =,][PAGE=,];

Web Management Location

System Administration > SS7 > SS7 Monitor Links > Stats

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

MSMLP; MSMLP:RESET=Y; MSMLP:PAGE=2;

Output Format

```
SS7 Monitor Link Measurements (Page 1 of 2)
MLINK     RXOCT   RXMSU  PERIOD
0         3333    822  00:12:00
1         0       0  00:12:00
Monitor Link Measurements (Page 2 of 2)
MLINK FFRAME FRAME  MFRAME LFRAME ABORT  CRC     DISC   RBUSY  PERIOD
0     22     375    8220   16320  124306 0       0      3      00:12:00
1     0      0      333    4343   1233   434126 0      0      00:12:00
```

The meaning of each field in the output is as follows:

- MLINK - Monitor link
- RXOCT - Number of Signaling Information Field (SIF) and Service Information Octets received
- RXMSU - Number of message signaling units octets received
- PERIOD - Time since measurements on the port were last reset.
- FFRAME - The number of (error-free) frames received, excluding any duplicate frames discarded as a result of the internal filtering mechanism.
- FRAME - The total number of (error-free) frames received including any duplicate frames discarded as a result of the internal filtering mechanism.
- MFRAME - The number of misaligned frames received.
- LFRAME - The number of received frames that were designated as either too long or too short for a configured protocol.
- ABORT - The number of aborts received.
- CRC - Number of CRC errors received.
- DISC - The number of times that the receiver discarded incoming frames as a result of no internal buffers being available. This is a count of the number of events rather than a count of the number of frames discarded.
- RBUSY - The number of times the receiver has entered the busy state as a result of the number of internal buffers falling below a set threshold.

6.11.13 MSNIP - Network Interface Measurements

This command displays traffic measurements for each Network Interface on the system taken over a period of time.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSNIP:[RESET=,][PAGE=];

Web Management Location

System Administration > Server Management > Network Interfaces > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSNIP;
MSNIP:RESET=Y,PAGE=2;

Output Format

```
Network Interface Measurements (Page 1 of 2)
NETIF    RXKBYTE RXPKT  RXERR  RXDROP TXKBYTE TXPKT  TXERR TXDROP PERIOD
eth0     0       0      0      0      0       0      0     0      16:34:41
eth1     96324   135705 0      4204E5 28169   4444   0     0      16:34:41
eth2     0       0      0      0      0       0      0     0      16:34:41
eth3     3760    3273   0      33615  12503   3455   0     0      16:34:41

Network Interface Measurements (Page 2 of 2)
NETIF RXFIFO  RXFRAME RXCOMP RXMULT TXFIFO TXCOLLS TXCARRIER TXCOMP PERIOD
0     0       0       0      0      0      0       0          0      16:34:41
1     0       0       0      0      0      0       0          0      16:34:41
2     0       0       0      0      0      0       0          0      16:34:41
3     0       0       0      0      0      0       0          0      16:34:41
```

Displayed values are as follows:

NETIF - Network Interface
RXKBTYE - Number of kilobytes of data received (in kilobytes).
RXPKT - Number of packets of data received.
RXERR - Number of receive errors detected.
RXDROP - Number of received packets dropped by the device driver.
TXKBTYE - Number of kilobytes of data transmitted (in kilobytes).
TXPKT - Number of packets of data transmitted.
TXERR - Number of transmit errors detected.
TXDROP - Number of transmit packets.
PERIOD - The measurement period the measurement was taken over.
RXFIFO - The number of FIFO buffer errors received.
RXFRAME - The number of packet framing errors received.
RXCOMP - The number of compressed packets received.
RXMULT - The number of multicast frames received.
TXFIFO - The number of FIFO buffer error transmitted.
TXCOLLS - The number of collisions detected on the transmit side.
TXCARRIER - The number of carrier losses detected on the transmit side.
TXCOMP - The number of compressed packets transmitted.

6.11.14 MSOGP - Message Router Origin Measurements

This command displays traffic measurements for Message Router Origins.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSOGP:[OGID=,][[RESET=];

Web Management Location

System Administration > Message Router > Origin > Stats

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MSOGP:OGID=4;

Output Format

```
Message Router Origin Measurements
OGID   RXMSU   RXOCT   DROPMSU DROPOCT TXMSU   TXOCT   PERIOD
4      4343    153323  343     2540    4000    120783  01:17:45
```

The meaning of each field in the output is as follows:

OGID - The Origin Identifier.
RXMSU - Messages received from the Origin.
RXOCT - Number of octets for Messages received from the Origin.
DROPMSU - Messages from the Origin that do not match a Routing Key.
DROPOCT - Number of octets Messages from the Origin that do not match a Routing Key.
TKMSU - Messages from the Origin that match a Routing Key.
TKOCT - Number of octets for Messages from the Origin that that match a Routing Key.
PERIOD - Measurement collection period.

6.11.15 MSPCP - PCM Measurements

This command displays traffic measurements for PCMs.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSPCP:[RESET=,];

Web Management Location

System Administration > Boards > PCMs > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSPCP; MSPCP:RESET=Y;

Output Format

```
PCM Measurements
PORTID PCM FMSLIP OUTSYN ERRSEC SEVSEC BITERR CV     PERIOD
1      1-3 57     60     23     1      0      0      23:00:00
2      1-4 12     35     33     4      0      0      01:00:00
3      2-3 53     55     4      0      0      0      01:00:00
```

The meaning of each field in the output is as follows:

- PORTID - Port ID as configured in config.txt file
- PCM - PCM on a board
- FMSLIP - Frame Slip count
- OUTSYN - Out-sync transitions
- ERRSEC - Errored Seconds count
- SEVSEC - Severely Errored Seconds count

- BITERR - A count of the actual number of bit errors detected by the framer device for the LIU. The precise meaning of this parameter varies depending on the operating mode of the framer:
  - — For E1 operating modes, it is the number of errors detected in the frame alignment word.
  - — For T1 interfaces operating in D3/D4 frame format, it is the number of framing bit errors.
  - — For T1 interfaces operating in ESF format, it is the number of CRC6 errors.

  Note: In general, the user should use the errored_seconds and severely_errored_seconds parameters instead since these parameters provide normalized values that have the same meaning for all modes of operation.
- CV - A count of all the line code violations detected on the interface.
- PERIOD - Time since measurements on the port were last reset.

6.11.16 MSRAP - SIGTRAN Remote Application Server Measurements

This command displays traffic measurements for Remote Application Servers.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSRAP:[RAS=,][[RESET=];

Web Management Location

System Administration > SIGTRAN > Remote Servers > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSRAP:RAS=4;

Output Format

```
Remote Application Server Measurements
RAS TXPKT  NOOS   PERIOD
4   4343   0      01:17:45
```

The meaning of each field in the output is as follows:

- RAS - The Remote Application Server identifier.
- TXPKT - M3UA Packets transmitted.
- NOOS - Number of times the RAS was Inactive or there were insufficient ASPs.
- PERIOD - Measurement collection period.

6.11.17 MSRKP - Message Router Routing Key Measurements

This command displays traffic measurements for Message Router Routing Keys.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSRKP:[RKI=,][[RESET=];

Web Management Location

System Administration > Message Router > Routing Key > Stats

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

MSRKP:RKI=4;

Output Format

```
Message Router Routing Key Measurements
RKI     RXMSU    RXOCT    DROPMSU DROPOCT BAKMSU  BAKOCT  TXMSU    TXOCT    PERIOD
4       4343     153323   343     2540    0       0       4000     120783   01:17:45
```

The meaning of each field in the output is as follows:

RKI - The Routing Key Index.
RKMSU - Messages received that match the Routing Key.
RKOCT - Number of octets for Messages received that match the Routing Key.
DROPMSU - Messages that match the Routing Key dropped.
DROPOCT - Number of octets Messages that match the Routing Key dropped.
BAKMSU - Messages that match the Routing Key passed to the partner Server.
BAKOCT - Number of octets Messages that match the Routing Key passed to the partner Server.
TXMSU - Messages that match the Routing Key transmitted to the destination.
TXOCT - Number of octets for Messages that match the Routing Key transmitted to the destination.
PERIOD - Measurement collection period.

6.11.18 MSRLP - Remote Server Link Measurements

This command displays traffic measurements for links to a remote Signaling. Server.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSRLP:[RESET =,];

Web Management Location

System Administration > Server Management > Dual Operation > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSRLP; MSRLP:RESET=Y;

Output Format

```
Remote SIU Link Measurements
LINKID TXMSG   RXMSG   TXOCT   RXOCT   OOSDUR NOOS    NDISCARD PERIOD
    1 1.43E6 1.45E6 5.48E6 5.35E6     62    1           0 00:14:55
```

The meaning of each field in the output is as follows:

- RXMSG - number of messages received.
- TXMSG - number of messages transmitted.
- RXOCT - number of octets received in messages excluding message header octets (rounded down to the nearest 1000).
- TXOCT - number of octets transmitted in messages excluding message header octets (rounded down to the nearest 1000).
- OOSDUR - the total amount time the link was out of service (in multiples of 100ms).
- OOSDUR - the total amount time the link was out of service (in multiples of 100ms).
- NOOS - the number of times the link went out of service.
- NDISCARD - the number of messages due to be transmitted that were discarded.
- PERIOD - the time period over which these statistics have been gathered (in hours, minutes and seconds).

6.11.19 MSSLP - SS7 Link Measurements

This command displays traffic measurements for SS7 links.

When measurements are reset values and the measurement period are set to zero.

Note: Page 1 and Page 2 Link statistics are reset using the RESET parameter.

Note: Page 3 Link statistics report Link utilization. For TDM links, the percentage utilization is expressed as a percentage of the available bandwidth. For M2PA links, this figure is expressed as the number of link equivalents.

Syntax

MSSLP:[RESET =,];

Web Management Location

System Administration > SS7 > SS7 Links > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSSLP;

MSSLP:RESET=Y;

Output Format

```
SS7 Link Measurements (Page 1 of 3)
LINK OOSDUR RXNACK RXMSU RXOCT TXMSU TXOCT  RTXOCT NCONG PERIOD
0    0      0      375   8220  16320 124306 0      0     00:12:00
1    0      0      392   8624  17036 141860 0      0     00:12:00
SS7 link measurements (page 2 of 3)
LINK ALIGN   SUERR   TBUSY   TCONG   TXDISCARD NEVENT  PERIOD
0    0       0       0       0       0         0       00:12:00
1    0       0       0       0       0         0       00:12:00
SS7 link measurements (page 3 of 3)
LINK  NR5M   NR1H   NR1D   OR5M OR1H OR1D NT5M   NT1H   NT1D   OT5M OT1H OT1D
0     0      0      0      0    0    0    0      0      0      0    0    0
1     0      0      0      0    0    0    0      0      0      0    0    0
```

The meaning of each field in the output is as follows:

LINK - SS7 signaling link.

OOSDUR - duration that the link was not in service.

RXNACK - number of negative acknowledgements received. Not applicable for IP-based SS7 links.

RXMSU - number of message signaling units octets received.

RXOCT - number of signaling Information Field (SIF) and Service Information Octet (SIO) octets received.

TXMSU - number of message signaling units octets transmitted.

TXOCT - number of SIF and SIO octets transmitted.

RTXOCT - octets retransmitted.

NCONG - congestion counter.

PERIOD - time since measurements on the link were last reset.

ALIGN - number of failed signaling link alignment attempts.

SUERR - number of signal units in error.

TBUSY - duration of local busy condition.

TCONG - duration of Link congestion.

TXDISCARD - number of MSUs discarded due to congestion.

NEVEN - number of congestion events leading to MSU discard.

NR5M - peak rate of MSUs received during the last 5 minutes (msu/s).

NR1H - peak rate of MSUs received during the last hour (msu/s).

NR1D - peak rate of MSUs received during the last day (msu/s).

OR5M - percentage 5 mins peak link receive utilization in a 10s period.

OR1H - Percentage 1 hour peak link receive utilization in a 10s period.

OR1D - Percentage 1 day peak link receive utilization in a 10s period.

NT5M - Peak rate of MSUs transmitted during the last 5 minutes (msu/s).

NT1H - Peak rate of MSUs transmitted during the last hour (msu/s).

NT1D - Peak rate of MSUs transmitted during the last day (msu/s).

NT1D - peak rate of MSUs transmitted during the last day (msu/s).

OT5M - percentage 5 mins peak link transmit utilization in a 10s period.

OT1H - percentage 1 hour peak link transmit utilization in a 10s period.

OT1D - percentage 1 day peak link transmit utilization in a 10s period.

6.11.20 MSSRP - SIGTRAN Route Measurements

This command displays traffic measurements for SIGTRAN Routes.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSSRP:[SNRT=,][[RESET=];

Web Management Location

System Administration > SIGTRAN > Routes > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSSRP:SNRT=4;

Output Format

```
SIGTRAN Route Measurements
SNRT TXPKT  NOOS   PERIOD
4    4343   0      01:17:45
```

The meaning of each field in the output is as follows:

- SNRT - The SIGTRAN Route identifier.
- TXPKT - M3UA Packets transmitted.
- NOOS - Number of times the Route was down.
- PERIOD - Measurement collection period.

6.11.21 MSSTP - SIGTRAN Link Measurements

This command displays traffic measurements for SIGTRAN links. The first page displays traffic measurements at the SCTP level and the second page display measurements for M3UA links.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSSTP:[SNLINK=,][PAGE=][SNTYPE=][RESET=];

Web Management Location

System Administration > SIGTRAN > Links > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSSTP:SNLINK=4;

Output Format

```
SIGTRAN Link Measurements (Page 1 of 2)
SNLINK SNTYPE   RXCK   TXCK   RTXCK  NOOS   OOSDUR PERIOD
4      SCTP     4117   4875   0      0      0      01:17:45

SIGTRAN Link Measurements (Page 2 of 2)
SNLINK SNTYPE   RXPKT  TXPKT  NOOS   PERIOD
4      M3UA     4343   4444   0      01:17:45
```

The meaning of each field in the output is as follows:

- SNLINK - the SIGTRAN link identifier.
- SNTYPE- the type of link measurements (SCTP M3UA).
- RXCK - SCTP Data chunks received.
- TXCK - SCTP Data chunks transmitted.
- RTXCK - SCTP Data chunks retransmitted.
- NOOS - number of times the SCTP/M3UA link is out of service/down.
- OOSDUR - total seconds the SCTP links was out of service.
- RXPKT - M3UA Packets received.
- TXPKT - M3UA Packets transmitted.
- PERIOD - measurement collection period.

6.11.22 MSSYP - System Measurements

This command displays system related measurements for load and congestion taken over a period of time.

When measurements are reset values and the measurement period are set to zero.

Syntax

MSSYP:[RESET=Y];

Web Management Location

System Administration > Server Management > System > Stats

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

MSSYP;

Output Format

```
System Measurements
NOVLD     0
MAX_LOAD  28.81%
LOADAVG   2.28%
PERIOD    18:36:55
```

The meaning of each field in the output is as follows:

- NOVLD - the number of periods of overload.
- MAX_LOAD - maximum load average measurement taken over 1 minute.
- LOADAVG - the average load on the system.
- PERIOD - the period the measurement was taken over.

6.11.23 MSHRP - MAP HLR Rx Measurements

Command to display traffic measurements for Receive MAP HLR Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified, Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSHRP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > HLR > HLR Rx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSHRP;

MSHRP:PAGE=2;

MSHRP:PROFILE=2;

MSHRP:RESET=Y;

Output Format

MAP HLR Rx Services Measurements (Page 1 of 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Rx_Send_Routing_Info_for_SM 0 0 01:29:16

Rx_Report_Delivery_SM 0 0 01:29:16

Rx_Atomic_Mobile_Term_TX_Req 0 0 01:29:16

Rx_Get_IMSI 0 0 01:29:16

Rx_Location_Request 3434 0 01:29:16

Rx_Subscriber_State_Reqs 1231 0 01:29:16

MAP HLR Rx Services Measurements (Page 2 of 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Rx_Send_Routing_Info_for_SM 0 0 01:29:16

0 Rx_Report_Delivery_SM 0 0 01:29:16

0 Rx_Atomic_Mobile_Term_TX_Req 0 0 01:29:16

0 Rx_Get_IMSI 0 0 01:29:16

0 Rx_Location_Request 3434 0 01:29:16

0 Rx_Subscriber_State_Reqs 1231 0 01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with a MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.24 MSHTP - MAP HLR Tx Measurements

Command to display traffic measurements for Transmit MAP HLR Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified, Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSHTP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > HLR > HLR Tx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSHTP;

MSHTP:PAGE=2;

MSHTP:PROFILE=2;

MSHTP:RESET=Y;

Output Format

MAP HLR Tx Services Measurements (Page 1 of 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Tx_Alert_SC 0 0 01:29:16

MAP HLR Tx Services Measurements (Page 2 of 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Tx_Alert_SC 0 0 01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with a MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.25 MSORP - MAP MO-SMS Rx Measurements

Command to display traffic measurements associated with MAP Received MO-SMS Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSORP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Rx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSORP;

MSORP:PAGE=2;

MSORP:PROFILE=2;

MSORP:RESET=Y;

Output Format

MAP MO-SMS Rx Measurements (Page 1 or 2)

MAP_SERVICE	SUCCESS	FAIL	PERIOD
Mobile_Orig_RX_Req	23	1	01:29:16
Alert_SC	0	0	01:29:16

MAP MO-SMS Rx Measurements(Page 2 or 2)

PROFILE	MAP_SERVICE	SUCCESS	FAIL	PERIOD
0	Mobile_Orig_RX_Req	23	1	01:29:16
0	Alert_SC	0	0	01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.26 MSOTP - MAP MO-SMS Tx Measurements

Command to display traffic measurements associated with MAP Transmit MO-SMS Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSOTP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MO-SMS Tx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSOTP;

MSOTP:PAGE=2;

MSOTP:PROFILE=2;

MSOTP:RESET=Y;

Output Format

MAP MO-SMS Tx Measurements (Page 1 or 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Mobile_Orig_TX_Req 23 1 01:29:16

MAP MO-SMS Tx Measurements(Page 2 or 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Mobile_Orig_TX_Req 23 1 01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.27 MSRTP - MAP Ready for SM Tx Profile Measurements

Command to display traffic measurements associated with MAP Ready for SM Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSRTP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > Ready for SM > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSRTP;

MSRTP:PAGE=2;

MSRTP:PROFILE=2;

MSRTP:RESET=Y;

Output Format

MAP Ready for SM Measurements (Page 1 or 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Ready_for_SM 3434 0 01:00:00

MAP Ready for SM Measurements(Page 2 or 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Ready_for_SM 3434 0 01:00:00

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.28 MSSPP - MAP Subscriber Profiling Measurements

Command to display traffic measurements associated with MAP Subscriber Profiling Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSSPP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > Subscriber > Subscriber > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSSPP;

MSSPP:PAGE=2;

MSSPP:PROFILE=2;

MSSPP:RESET=Y;

Output Format

MAP Subscriber Profiling Measurements(Page 1 of 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Location_Request 3434 0 01:00:00

Subscriber_State_Reqs 1231 0 01:00:00

Get_IMSI 0 0 01:00:00

MAP Subscriber Profiling Measurements (Page 2 of 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Location_Request 3434 0 01:00:00

0 Subscriber_State_Reqs 1231 0 01:00:00

0 Get_IMSI 0 0 01:00:00

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.29 MSTRP - MAP MT-SMS Rx Measurements

Command to display traffic measurements associated with a MAP Receive MT-SMS service profile.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSTRP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Rx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSTRP;

MSTRP:PAGE=2;

MSTRP:PROFILE=2;

MSTRP:RESET=Y;

Output Format

MAP MT-SMS Rx Measurements (Page 1 or 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Mobile_Term_RX_Req 23 1 01:29:16

MAP MT-SMS Rx Measurements (Page 2 or 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Mobile_Term_RX_Req 23 1 01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.30 MSTTP - MAP MT-SMS Tx Measurements

Command to display traffic measurements associated with MAP Transmit MT-SMS Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSTTP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > SMS > MT-SMS Tx > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSTTP;

MSTTP:PAGE=2;

MSTTP:PROFILE=2;

MSTTP:RESET=Y;

Output Format

MAP MT-SMS Tx Measurements (Page 1 or 2)

MAP_SERVICE SUCCESS FAIL PERIOD

Mobile_Term_TX_Req 23 1 01:29:16

Send_Routing_Info_for_SM 0 0 01:29:16

Report_Delivery_SM 0 0 01:29:16

Atomic_Mobile_Term_TX_Req 0 0 01:29:16

MAP MT-SMS Tx Measurements (Page 2 or 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 Mobile_Term_TX_Req 23 1 01:29:16

0 Send_Routing_Info_for_SM 0 0 01:29:16

0 Report_Delivery_SM 0 0 01:29:16

0 Atomic_Mobile_Term_TX_Req 0 0 01:29:16

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.11.31 MSUPP - MAP USSD Measurements

Command to display traffic measurements associated with MAP USSD Services.

Page 1 displays summary measurements associated with each MAP service.

Page 2 displays measurements for each profile associated with a MAP service.

When a profile is specified Page 2 measurements are displayed.

When measurements are reset, values and the measurement period are set to zero. Individual profile measurements are only reset when the profile ID is specified as well as the reset field; otherwise, the counters for the per service measurement summary are reset.

Syntax

MSUPP:[RESET=,][PAGE=,|PROFILE=,];

Web Management Location

System Administration > MAP Services > USSD > USSD > Stats

Applicability

Operating Modes: SWS

Permissions: Configuration Read Access

Example

MSUPP;

MSUPP:PAGE=2;

MSUPP:PROFILE=2;

MSUPP:RESET=Y;

Output Format

MAP USSD Measurements (Page 1 or 2)

MAP_SERVICE SUCCESS FAIL PERIOD

USSD_Mobile_Init_Sessions 55 4 01:00:00

USSD_App_Init_Sessions 44 1 01:00:00

USSD_Notify_Request 54345 0 01:00:00

MAP USSD Measurements(Page 2 or 2)

PROFILE MAP_SERVICE SUCCESS FAIL PERIOD

0 USSD_Mobile_Init_Sessions 55 4 01:00:00

0 USSD_App_Init_Sessions 44 1 01:00:00

0 USSD_Notify_Request 54345 0 01:00:00

The meaning of each field in the output is as follows:

PROFILE - a profile associated with the MAP service.

MAP_SERVICE - the MAP service.

SUCCESS - count of successes.

FAIL - count of failures.

PERIOD - time since measurements for the service were last reset.

6.12 Reset Commands

“RSBOI - Restart Board Initiate”

6.12.1 RSBOI - Restart Board Initiate

This command will restart a board. The board will be re-configured from the system configuration data.

Syntax

RSBOI:BPOS=;

Web Management Location

System Administration > Boards > Boards > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: System Maintenance Access

Prerequisites

The board must have already been initialized.
There are no startup parse or configuration errors present.
There are no restart or configuration failed alarms present in the alarm log.

Example

RSBOI:BPOS=1;

6.13 Status Commands

"STBOP - Board Status"

"STCGP - Circuit Group Status"

"STCRP - SS7 Route Status"

"STDDP - Disk Drive Status"

"STDEP - Circuit Group Device Status"

"STDHP - Status DTS Host Print"

"STHLP - Host Link Status"

"STIPP - IP Node Status"

"STLCP - Software License Capability Status"

"STMLP - SS7 Monitor Link Status"

"STNIP - Network Interface Status"

"STPCP - PCM Status"

"STRAP - SIGTRAN Remote Application Server Status"

"STRLP - Remote Server Link Status"

"STSLP - SS7 Link Status"

"STSRP - SIGTRAN Route Status"

"STSSP - SCCP Subsystem Resource Status"

"STSTP - SIGTRAN Signaling Link Status"

"STSWP - System Software Status"

"STSYP - System Status"

"STTDP - TCAP Dialogue Status"

"STTPP - NTP Server Status"

"STTRP - TCAP Resource Status"

"STUAP - User Account Status"

6.13.1 STBOP - Board Status

This command displays the status of all configured signaling boards.

Syntax

STBOP;

Web Management Location

System Administration > Boards > Boards > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STBOP;

Output Format

```
Board status
  BPOS       BRDTYPE    SERIAL_NUMBER       BRD_STATUS
  0          SS7MD      PX8000001           ACTIVE
  1          SS7MD      PX8000002           ACTIVE
```

The parameters have the following meanings:

- BPOS - Board position
- BRDTYPE - Board type. Possible board types are : SS7LD or SS7MD
- SERIAL_NUMBER - The serial number of the board. If a board is replaced or a new board added then the board type should be set/changed on the board configuration command and the system restarted after which it will extract the new serial number of the board.
- BRD_STATUS - The state the board is in. Possible state values are INACTIVE, RESETTING, ACTIVE, FAILED

6.13.2 STCGP - Circuit Group Status

This command displays the status of the configured circuit groups.

Syntax

STCGP:[GID=];

Web Management Location

System Administration > Call > Circuit Groups > Status

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STCGP; STCGP:GID=2;

Output Format

```
Circuit group status
GID GTYPE CICS MAINT CCTACT IDLE
0   S    30   0     0      30
1   S    INACTIVE
2   S    15   3     5      7
3   S    INACTIVE
```

The meaning of each field in the output is as follows:

- GTYPE - Reserved for future use; displays "S" by default.
- CICS - The number of Circuits assigned to the circuit group. If the group was configured but not activated an INACTIVE indication is shown and all other parameters on the row are blank.
- MAINT - The number of circuits that do not have calls in progress and have an active maintenance state (and therefore are not available for selection).
- CCTACT - The number of circuits that have calls in progress.
- IDLE - The number of circuits that do not have calls in progress, but are available for selection.

6.13.3 STCRP - SS7 Route Status

This command shows the status of all configured SS7 routes.

Syntax

STCRP:[C7RT=];

Web Management Location

System Administration > SS7 > SS7 Routes > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STCRP;

Output Format

```
C7RT  NC     DPC   C7RT_STATUS CONG_LEVEL LS1_STATUS  LS2_STATUS
1     NC0    1021  Available   0          Available
2     NC0    2171  Available   0          Available   Available
3     NC1    51    Unavailable 0          Unavailable
```

The meaning of each field in the output is as follows:

- ROUTE - Logical reference for an SS7 route
- NC - SS7 Network Context
- ROUTE STATUS - Possible values are:
  - — Available - The route is available for traffic to the remote point code of the route.
  - — Unavailable - The route is unavailable for traffic to the remote point code of the route.
- CONG LEVEL - Possible values are:
  - — 0, no congestion
  - — 1, 2, or 3 indicates the ITU/ANSI congestion level

- LS1 STATUS and LS2 STATUS - Possible values are:
  - — Available - The link set on the route is available for traffic to the adjacent point code.
  - — Unavailable - The link set on the route is unavailable for traffic to the adjacent point code.

6.13.4 STDDP - Disk Drive Status

This command displays the status of all hard disk drives within the RAID array.

Syntax

STDDP;

Web Management Location

System Administration > Server Management > Disk Drives > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STDDP;

Output Format

```
Disk Drive status
DRIVE STATE
1     UP
2     UP
```

The STATUS field will display one of the following values:

- UP – The disk drive is operational and all the RAID devices on this drive are in an active sync state
- DOWN – The disk drive is non operational as one or more of the Raid devices on this drive is faulty.
- RESTARTING – One or more of the raid devices on this drive is synchronizing with another Raid device. The disk is considered non operational until synchronization is complete.
- INACTIVE – The drive is not configured as part of the RAID array and therefore is not in use. This may be due to user action through MMI, the drive not being physically present at startup or a failed drive being removed by the operating software at start up from the RAID array.

Caution: Before replacing a failed drive, the drive must first be taken out of service using the MNINI command. Once the replacement drive is in place, the disk can be restored to service using the MNINE command.

6.13.5 STDBP – Subscriber Database Service Status

This command displays status associated with Subscriber Database Services.

Syntax

STDBP;

Web Management Location

System Administration > Subscriber Database > Services > Status

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STDBP;

Output Format

Subscriber Database Service Status

DBSVCTYPE MNP

DBSVCID 5

DB0 0-PRI

DB1 3-FAILED

DB2 4-PRI

DB3 5-PRI

DB6 1-FAILED

DB7 2-SEC

The meaning of each field in the output is as follows:

DBSVCID – the Service ID.

DBSVCTYPE – the Service type.

DB0..DB15 – the status of the database via each host. The parameter is a compound parameter of the form x-y where x is an SIU Host ID and y may be one of the following.

PRI - the database is available and part of the primary pool.

SEC – the database is available and part of the secondary pool.

FAILED - the database is not currently accessible.

6.13.6 STDEP - Circuit Group Device Status

This command displays the status of all circuits within the circuit group. Refer to the associated protocol programmer's manual for a complete list of returned status values.

Syntax

STDEP:GID=,;

Web Management Location

System Administration > Call > Circuit Groups > Status

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STDEP:GID=3;

Output Format

```
  Circuit Group Device Status
  GID   CID     CIC     HEX   PROTOCOL_STATUS  BLOCKING_STATUS
  3     1       32      0x04  IC_CONNECT       --------
  3     2       33      0x02  IC_W_ACM         --------
  3     3       34      0x00  IDLE             ----LM--
  3     4       35      0x00  IDLE             --------
```

The meaning of each field in the output is as follows:

- GID - Circuit group identifier.
- CID - Circuit identifier.
- CIC - Circuit identification code.
- HEX - Hexadecimal status value.
- PROTOCOL STATUS - Abbreviated status text.
- BLOCKING STATUS -
- LH - Circuit is locally hardware blocked.
- RH - Circuit is remotely hardware blocked.
- LM - Circuit is locally maintenance blocked.
- RM - Circuit is remotely maintenance blocked.

6.13.7 STDHP - Status DTS Host Print

As a result of changes to DTS, the STDHP command has changed and is now defined as follows:

Synopsis

This command displays the routing availability status of DTS hosts.

If NC and SSN are blank then the output shows routing availability for all the LSS configured.

If NC only is supplied then the output shows routing availability for all the LSS associated with the specified NC.

If NC and SSN are supplied then the output shows routing availability for the specified NC and SSN.

If the subsystem number is not found in the DTS routing requests but a default routing request for the NC exists, the status of hosts associated with the default routing for that NC is displayed with the Routing Method shown as "Default", rather than "Explicit".

If no DTS routing requests exist for the NC then the status of all DTS hosts is displayed.

The RT_MATCHED field has three values:

- Where a match with a default routing request exists it will be "Default".
- Where a match with an explicit (NC and SSN) routing request exists it will show "Explicit".
- Where no routing request is applicable it will show "None" for all hosts and host routing selection will be by availability only.

Syntax

STDHP:NC=;
STDHP:NC=,SSN=,;

Web Management Location

System Administration > Transaction > DTS Hosts > Status

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STDHP;

Output Format

```
DTS Host Status
NC   SSN DRID HOSTID RT_MATCHED  HOST_SELECTION STATUS
NC0      0    1      Default     Strict         ACTIVE
NC0 4    0    1      Default     Strict         ACTIVE
NC0 5    1    2      Explicit    Strict         SHUTDOWN PREPARE
NC0 8    2    0      Explicit    Strict         ACTIVE
NC1           0      None        Strict         ACTIVE
NC1           1      None        Strict         ACTIVE
NC1           2      None        Strict         SHUTDOWN PREPARE
NC1 5         0      None        Strict         ACTIVE
NC1 5         1      None        Strict         ACTIVE
NC1 5         2      None        Strict         SHUTDOWN PREPARE
```

6.13.8 STFEP - Flow Environment Status

This command requests the status of the Flow Environment.

Syntax

STFEP;

Web Management Location

System Administration > Diagnostics > Flow Environment > Status

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

STFEP;

Output Format

```
Flow Environment Status
QCUR   4343
QMAX   4000
```

6.13.9 STHPP - Diameter Peer Status

This command requests the status of Diameter peers.

Syntax

STHPP:[HDPR=];

Web Management Location

System Administration > Diameter > Peer > Status

Applicability

Operating Modes: DSH

Permissions: Configuration Read Access

Example

STHPP;

STHPP:HDPR=0;

Output Format

```
Diameter Peer Status
HDPR   RSP_STATUS   TINSTATE TACTIVE
1      AVAILABLE    01:17:45 01:17:45
```

6.13.10 STHLP - Host Link Status

This command displays the status of all configured Host Links.

Syntax

STHLP;

Web Management Location

System Administration > DSI Hosts > Hosts > Status

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STHLP;

Output Format

```
Host SIU Link Status
HOSTID MHOST RSI_STATUS LOCAL_IPADDR       REMOTE_IPADDR
0      *     FAILED
1            ACTIVE     192.168.0.126:9000 192.168.0.126:39005
```

A * indicates that a host is acting as a management host.

Possible RSI_STATUS values are : ACTIVE, FAILED, DEACTIVATED.

6.13.11 STIPP - IP Node Status

This command sends five ICPM (Internet Control and Management Protocol) Echo Request frames to the specified remote IP address. The command will output the route the frame takes reporting statistics for each node on the journey.

Syntax

STIPP:PING_IPADDR=;

Web Management Location

System Administration > Diagnostics > Ping IP Address > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STIPP:PING_IPADDR=192.168.0.126;

Output Format

```
IP Node Status
PING_IPADDR      LOSS_PCT   LAST_PING  AVG_PING   BEST_PING  WORST_PING DEV_PING
192.168.1.104    0.0%       1.2        14.0       1.2        39.2       21.9
```

The meaning of each field in the output is as follows:

IPADDR - The IP address of each node in a route to an IP Destination (the last IPADDR shown) to which five ICPM Echo Request frames are to be sent.

LOSS_PCT - The percentage of packets lost.

LAST_PING - The time in milliseconds the last ping took to reach and return from the target IP node.

AVG_PING - The average time in milliseconds the set of pings took to reach and return from the target IP node.

BEST_PING - The time in milliseconds the best ping took to reach and return from the target IP node.

WORST_PING - The time in milliseconds the worst ping took to reach and return from the target IP node.

DEV_PING - The standard deviation of the time in milliseconds the pings took to reach and return from each the target IP node.

6.13.12 STLCP - Software License Capability Status

This command shows the status of software licenses on the system.

Note: The maximum account credit is the licensed throughput rate * 30. The throughput account credit is decremented each time traffic passes through the system. The throughput account credit is incremented every second by the value of the licensed throughput rate. If the licensed throughput is exceeded for a sustained period of time the credit available will drop. When the credit drops to 50% of the maximum throughput credit a congestion alarm will activate When the credit drops to 0% (i.e., there is no credit left a throughput enforcement alarm will be activated and throughput will be limited to the licensed rate). Throughput enforcement will be maintained until the account credit returns to 75% or above of the maximum throughput credit.

Syntax

STLCP;

Web Management Location

System Administration > Software > Software Licenses > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STLCP;

Output Format

```
Software License Capability Status
CAPABILITY   EVALUATION   NC  STATUS       LINKS   RATE    CREDIT
SIU                          ACTIVE
SWS                          INACTIVE
M2PA                         ACTIVE
M3UA                     NC0  ACTIVE       16      154     100
MTP                          ACTIVE
TCAP                         ACTIVE
MAP                          ACTIVE
IS41                         DEACTIVATED
INAP                         INACTIVE
SNMP                         ACTIVE
MONITORING                   ACTIVE
```

The meaning of each field in the output is as follows:

- CAPABILITY – A Licensable capability of the system. This is a protocol or operating mode capability which has been purchased or is under evaluation.
- EVALUATION - A * indicates that the license capability is undergoing evaluation.
- NC - A Network Context the capability is associated. Blank if not applicable.
- STATUS - State of the license capability on the system where:
- NONE - This capability is not present. It requires a software license.
- INACTIVE - The license is present but not running for software reasons (e.g., the license is for a different mode of operation or the capability is dependent on another capability that is not active).
- DEACTIVATED - The license is present but not running due to configuration reasons.

- ACTIVE - The license is active.
- ERROR - This license cannot be activated as it depends on another license which is not present (e.g., TCAP is present but SCCP is not).
- CONGESTED - The throughput congestion level has been reached for the capability.
- ENFORCE - The licensed traffic rate has been exceeded for a extended period and the system is now limiting traffic to the licensed rate for the capability.

  Note: If the status is preceded with a "*" the license is not present but as the system is currently operating without a license the functionality is available to the user. After one hour the system will restart and this functionality will again be deactivated as it is not licensed.
- LINKS - The available number of links for the capability. Blank means not applicable. For TDM the available links may be less than the licensed number of links if the share is being split with SIGTRAN.
- The share is controlled using the TDM share parameter on the system configuration command.
- RATE - The available throughput rate in Kilobyte/s for the capability. Blank means not applicable. The available throughput may be less than the licensed number if its share is being split with TDM or between M2PA and M3UA. This share is controlled using the TDM and M3UA share parameters.
- CREDIT - The current throughput account credit if applicable. The throughput account credit is expressed as a percentage of the maximum account credit.

6.13.13 STMLP - SS7 Monitor Link Status

This command displays the status of configured SS7 Monitor links. If the LINK parameter is specified, the status of the corresponding link is displayed. If the LINK parameter is not specified, the status of all configured Monitor links is displayed.

Syntax

STMLP:[MLINK=,];

Applicability

Operating Modes: SIU

Permissions: Configuration Read Access

Example

STMLP;

Output Format

```
SS7 Monitor Link Status
MLINK  L2_LINK_STATUS
0      OUT OF SERVICE
1      IN SERVICE
2      IN SERVICE
```

The meaning of each field in the output is as follows:

- MLINK - Shows the value of the link_id parameter for that link as configured using the MONITOR_LINK command in the config.txt file.
- LINK_STATUS - Layer 2 status; possible values are:
- NOT APPLICABLE - Status is not applicable for this type of monitor link.

- UNKNOWN - No traffic is being observed by the monitor link.
- OUT OF SERVICE - The monitored link appears out of service.
- IN SERVICE - The monitored link appears in service.

6.13.14 STNIP - Network Interface Status

Reports the status of the Network interfaces.

Syntax

STNIP;

Web Management Location

System Administration > Server Management > Network Interfaces > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STNIP;

Output Format

```
Network Interface Status (Page 1 of 2)
NETIF   SPEED DUPLEX STATUS
ETH0    100   FULL   UP
ETH1    100   FULL   UP
ETH2                 DOWN
ETH3                 DOWN

Network Interface Status (Page 2 of 2)
NETIF     ADDR_TYPE       IPADDR
BOND0     STATIC_IPV4     173.28.148.240/24
BOND0     STATIC_IPV6     fe77:19a9:8cf0:148:215:b2ff:fea1:f8ac/64
ETH0      LOCAL_IPV6      fe80::21b:63ff:feab:e6a6
ETH1      LOCAL_IPV6      fe80::21b:63ff:feab:e6a7
ETH2      LOCAL_IPV6      fe80::21b:63ff:feab:e6a8
ETH2      STATIC_IPV4     171.28.148.12/24
ETH3      STATIC_IPV4     fe80::21b:63ff:feab:e6a9
ETH3      LOCAL_IPV6      172.28.148.126/24
ETH3      STATIC_IPV6     fd77:19a9:8cf0:148:20e:cff:fec7:4b34/64
```

The meaning of each field in the output is as follows:

NETIF - The Network Interface name.

SPEED - The speed of the Network Interface in MHz (ETH only).

DUPLEX - Whether the interface is FULL or HALF duplex (ETH only).

STATUS - Whether the interface UP/DOWN .

IPADDR - Actual IP Addresses assigned to the network interface.

May IPV4, Global IPV6 or Link Local IPV6.

6.13.15 STPCP - PCM Status

This command displays the status of all configured PCM ports.

Syntax

STPCP;

Web Management Location

System Administration > Boards > PCMs > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STPCP;

Output Format

```
PCM status
  PORTID PCM SYNCPRI PCM_STATUS   CLOCK_STATUS
  0      0-3 *      OK           STAND ALONE
  2      1-1 1      OK           ACTIVE
  3      1-2 31     OK           OK
  5      1-4 0      BER > 1:10^5 FAULT
```

Possible STATUS values are: PCM LOSS, AIS, SYNC LOSS, REMOTE ALARM, BER > 1:10^3, BER > 1:10^5, OK

Possible CLOCK STATUS values are: FAULT, NOT OK, ACTIVE, OK, STAND ALONE (telephony bus disabled)

> ***Note:*** When the internal telephony bus is disabled in the board, the asterisk symbol (*) is displayed in the SYNCPRI field and the CLOCK STATUS is set to STAND ALONE.

Possible PCM STATUS values are:

- PCM LOSS - No signal sensed on the PCM input.
- AIS - The remote side sends all ones indicating that there is an error condition, or it is not initialized.
- SYNC LOSS - Loss of frame alignment since no frame synchronization has been received.
- REMOTE ALARM - The remote end indicates that is it is OK, but also indicates that it is detecting an error condition.
- BER > 1:10^3 - The PCM is encountering a Bit Error Rate (BER) of 10^3.
- BER > 1:10^5 - The PCM is encountering a BER of 10^5.
- OK - The PCM is operational.
- Possible CLOCK STATUS values are:
- FAULT - The PCM is unable to provide clock for the SIU due to a fault on the board.
- NOT OK - The PCM is not a valid clock source.
- ACTIVE - The PCM is a valid clock source and is currently providing clock for the server.
- OK - The PCM is a valid clock source but is currently not providing clock for the SIU.

- STANDBY - The PCM is a valid clock source and will provide clock for the server in the event of failure of the ACTIVE clock source.
- STAND ALONE - Telephony bus disabled.

6.13.16 STRAP - SIGTRAN Remote Application Server Status

This command displays the status of all links associated with the remote application server.

Syntax

STRAP:RAS=,;

Web Management Location

System Administration > SIGTRAN > Remote Servers > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STRAP:RAS=1;

Output Format

```
SIGTRAN Remote Application Server Status
RAS   NC   DPC       RC          SNLINK  AS STATUS     ASP STATUS  TRMD
1     NC0  401       1           1       AVAILABLE     ACTIVE      LS
```

The meaning of each field in the output is as follows:

- RAS - The remote application server identifier.
- NC - Network context.
- DPC - Destination point code.
- RC - Routing context.
- SNLINK - SIGTRAN link identifier.
- RAS_STATUS - Status of the remote application server. Definitions are:
- AVAILABLE - The RAS is available.
- UNAVAILABLE - The RAS is unavailable.
- INSUFF_ASP - The RAS is available but it has insufficient ASPs active as configured by the STN_RAS command (only valid for load sharing).
- ASP_STATUS - Status of the remote application server process. Definitions are:
- DOWN - The link attached to the server is down.
- ACTIVE - The link attached to the server is active.
- INACTIVE - The link attached to the server is inactive.
- TRMD - Traffic mode. Definitions are:
- LS - Load sharing mode.
- OR - Override mode.
- BC - Broadcast mode.

6.13.17 STRLP - Remote Server Link Status

This command displays the status of the configured Inter-SIU Ethernet links.

Syntax

STRLP;

Web Management Location

System Administration > Server Management > Dual Operation > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

MMI Prerequisites

The SIU must be a member of a dual pair.

Example

STRLP;

Output Format

```
Remote SIU Link Status
LINKID RSI_STATUS LOCAL_IPADDR       REMOTE_IPADDR
0      ACTIVE     192.168.0.126:9000 192.168.0.126:39005
```

Possible RSI_STATUS values are : ACTIVE, FAILED, DEACTIVATED.

6.13.18 STSLP - SS7 Link Status

This command displays the status of configured SS7 signaling links. If the LINK parameter is specified, the status of the corresponding link is displayed. If the LINK parameter is not specified, the status of all configured SS7 signaling links is displayed.

Syntax

STSLP:[LINK=,];

Web Management Location

System Administration > SS7 > SS7 Links > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSLP;

Output Format

```
SS7 Link Status
LINK   L3_STATUS      L3_STATUS    L3_BLOCKING_STATUS
0      OUT OF SERVICE UNAVAILABLE  ---- ---- ---- ---- ---- ---- ----
1      OUT OF SERVICE UNAVAILABLE  INHL INHR ---- ---- ---- ---- ----
2      OUT OF SERVICE UNAVAILABLE  INHL ---- ---- ---- ---- ---- ----
3      OUT OF SERVICE UNAVAILABLE  INHL ---- ---- ---- ---- ---- ----
4      IN SERVICE     AVAILABLE    ---- ---- ---- ---- CBIP ---- ----
5      IN SERVICE     AVAILABLE    ---- ---- ---- ---- ---- ---- LIIP
```

The meaning of each field in the output is as follows:

- LINK - Shows the value of the link_id parameter for that link as configured using the MTP_LINK command in the config.txt file.
- L2_STATUS - Layer 2 status; possible values are:
- IN SERVICE, OUT OF SERVICE, PROCESSOR OUTAGE, ALIGNED READY INITIAL ALIGNMENT, ALIGNED NOT RDY
- L3_STATUS - Layer 3 status; possible values are
  - AVAILABLE, UNAVAILABLE, CONGESTED, DEACTIVATED (the link has been deactivated by the user) or DOWN_NOHOST(the link has be taken down as there are no available hosts).
- L3_BLOCKING_STATUS - L3 Blocking Status; possible values are
- INHR - The Link is remotely inhibited
- INHL - The Link is locally inhibited.
- BLKR - The Link is Remotely Blocked
- COIP - Changeover is in progress
- CBIP - Changeback is in progress
- LIIP - Local Link inhibiting is in progress
- LUIP - Local Link unhibiting is in progress

6.13.19 STSRP - SIGTRAN Route Status

This command displays the status of SIGTRAN routes.

Syntax

STSRP:[SNRT=,];

Web Management Location

System Administration > SIGTRAN > Routes > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSRP; STSRP:SNRT=3;

Output Format

```
Status SIGTRAN Routes Print
SNRT     NC         DPC        SG    RT_STATUS        GW_STATUS
  1      NC3        401        2     AVAILABLE        AVAILABLE
```

The meaning of each field in the output is as follows:

- SNRT - The SIGTRAN route identifier.
- NC - Network context.
- DPC - Destination point code.
- SG - Signaling gateway identifier.
- RT_STATUS - Status of the signaling route. Definitions are
- AVAILABLE - The Point Code is available over this route.
- UNAVAILABLE - The Point Code is unavailable over this route.
- GW_STATUS - Status of the signaling gateway. Definitions are:
- AVAILABLE - The gateway is available.
- UNAVAILABLE - The gateway is unavailable.

6.13.20 STSSP - SCCP Subsystem Resource Status

This command displays the status of configured subsystems. If the ID parameter is specified, the status of the corresponding sub-system is displayed. If the ID parameter is not specified, the status of all configured subsystems is displayed.

Syntax

STSSP:[SSRID=,];

Web Management Location

System Administration > Transaction > SCCP SSRs > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSSP;

Output Format

```
SCCP Subsystem Resource Status
SSRID  NC        SSR      SSN   SPC       SSR_STATUS
3      NC0       RSS      12    3226      ALLOWED
4      NC1       RSP      -     3229      PROHIBITED
5      NC0       LSS      12    -         ALLOWED
```

The meaning of each field in the output is as follows:

- ID - Shows the SSR ID parameter of the subsystem as configured using the SCCP_LSS, SCCP_RSS or SCCP_RSP statements in the config.txt file.
- NC - Network context to which subsystem belongs.
- SSR - Type of SSR. Types are: LSS, RSS, RSP.
- SSN - The SubSystem Number of the subsystem.
- SSR_STATUS - The current state of the subsystem as returned by SCCP. Possible values are:
  - ALLOWED - The subsystem is available
  - PROHIBITED - The subsystem is not available

6.13.21 STSTP - SIGTRAN Signaling Link Status

Command to display the status of SIGTRAN links. Page 1 displays the status of the association while page 2 displays the individual status of each path in the association.

Syntax

STSTP:[SNLINK=,][SNTYPE=][PAGE=];

Web Management Location

System Administration > SIGTRAN > Links > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSTP;

Output Format

```
SIGTRAN Signaling Link Status (Page 1 of 2)
SNLINK  SNTYPE   RSP_STATUS   SCTP_STATUS
1       M3UA     AVAILABLE    ESTABLISHED


SIGTRAN Signaling Link Status (Page 2 of 2)
SNLINK  PATH_STATUS     RTO    CWND   SRTT   PMTU   REMOTE_IPADDR
1       ACTIVE          200    6000   3      1500   172.28.148.244
1       INACTIVE                                    173.28.148.244
```

The meaning of each field in the output is as follows:

SNLINK - the SIGTRAN link identifier.

SNTYPE - the type of link (M2PA, M3UA).

RSP_STATUS - Status of the M3UA remote signaling process or blank for M2PA.

SCTP_STATUS - SCTP association status.

PATH_STATUS - Primary, Active, Inactive, Invalid or Unconfirmed.

RTO - the SCTP retransmission timeout.

CWND - the current congestion window for the peer address.

SRTT - the current calculated smoothed round-trip time for the peer address in milliseconds.

PMTU - the current Path MTU for the peer address.

IPADDR - the remote IP address for the path.

6.13.22 STSWP - System Software Status

This command provides an overall summary of the software operating on the system.

Syntax

STSWP;

Web Management Location

System Administration > Software > System Software > Status Operations > Home Footer > Home

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSWP;

Output Format

```
System Summary
SYSTYPE     SIU
SOFTWARE    SS7G40-SIU Release 1.0.0 (Build 1001)
UNITID      000423a683bd
NODE        sysnode
SYSID
SYSREF      0
UPTIME      00:00:15
WARNING     2
MINOR       2
MAJOR       0
CRITICAL    0
```

6.13.23 STSYP - System Status

This command provides a summary of the load, uptime and alarms on the system.

Syntax

STSYP;

Web Management Location

System Administration > Server Management > System > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STSYP;

Output Format

```
System Status
CPU_MODEL   1 X Intel(R) Xeon(R) CPU E5504  @ 2.00GHz
MEMORY    3072MB
UPTIME    09:04:02
NRESTART  5
LOADAVG1  28.81%
LOADAVG5  2.28%
LOADAVG15 1.35%
ALMSYS    1
ALMPCM    0
ALMSIG    1
ALMCLA1   2
ALMCLA2   0
ALMCLA3   0
```

The meaning of each field in the output is as follows:

- CPU - A string identifying the CPU type and speed.
- MEMORY - The amount of RAM in the system.
- UPTIME - The length of time the application software has been running.
- NRESTART - The number of times the system has restarted since factory installation.
- LOADAVG1 - The load average measurement taken over 1 minute.
- LOADAVG5 - The load average measurement taken over 5 minutes.
- LOADAVG15 - The load average measurement taken over 15 minutes.
- ALMSYS - The number of system alarms.
- ALMPCM - The number of PCM alarms.
- SIG - The number of signaling alarms.
- ALMCLA1 - The number of minor alarms.
- ALMCLA2 - The number of major alarms.
- ALMCLA3 - The number of critical alarms

6.13.24 STTDP - TCAP Dialogue Status

This command allows the user to read the status of TCAP.

Syntax

STTDP:[DLGID=,RANGE=];

Web Management Location

System Administration > Transaction > TCAP Dialogs > Status

Applicability

Operating Modes: SIU, SWS

Permissions: Configuration Read Access

Example

STTDP:DLGID=122,RANGE=2;

Output Format

```
TCAP Dialogue Status
DLGID DHA    TSM    DCS    INVK LTRID    RTRID
123   ACTIVE ACTIVE ACTIVE 5    0000C040 0000C080
```

The meaning of each field in the output is as follows:

- DHA - TCAP dialog handler state. Possible values are: IDLE, RCVD, SENT, ACTIVE
- TSM - TCAP dialog transaction state. Possible values are: IDLE, RCVD, SENT, ACTIVE
- DCS - TCAP dialog control structure state. Possible values are: FREE, PENDING, ACTIVE, ISM
- INVK - Number of active invokes in dialog
- LTRID - Local transaction identity
- RTRID - Remote transaction identity

6.13.25 STTPP - NTP Server Status

This command displays the status of the Network Time Protocol servers configured.

Syntax

STTPP;

Web Management Location

System Administration > Server Management > NTP Servers > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STTPP;

Output Format

```
NTP Server Status
NTPSER IPADDR          STATUS      STRATUM NTP_OFFSET LABEL
1      192.168.0.1     SYSPEER     3       0.000321   Primary NTP server
2      192.168.0.2     ACTIVE      4       0.000232   NTP server 2
```

The STATUS reported in the output is as follows:

- INACTIVE - The NTP service is disabled.
- UNREACHABLE - The NTP server is unreachable.
- REJECT - The NTP server has been rejected by the server selection algorithm.
- ACTIVE - NTP time information is being received from this server.
- SYSPEER - NTP has selected this server to synchronize to.
- The STRATUM indicates the number of servers between the system NTP client and a reference clock.
- The NTP_OFFSET reported in the output is the Estimated difference in seconds between the system NTP Client and NTP Server.

6.13.26 STTRP - TCAP Resource Status

This command shows the status of TCAP resources.

Syntax

STTRP;

Web Management Location

System Administration > Transaction > TCAP Resources > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STTRP;

Output Format

```
TCAP Resource Status
ICD OGD   INVK  CPT   DBUF
122 12233 2222  222   22
```

The meaning of each field in the output is as follows:

- ICD - Number of active incoming dialogs
- OGD - Number of active outgoing dialogs
- INVK - Number of active invokes
- CPT - Number of allocated component structures. These are used temporarily for pending component requests until an appropriate dialog request is received.
- DBUF - Number of allocated dialog buffers. These are used temporarily for building dialog request messages from pending components.

6.13.27 STUAP - User Account Status

This command displays which users are logged on and where.

Syntax

STUAP;

Web Management Location

System Administration > Access Control > User Accounts > Status

Applicability

Operating Modes: SIU, SWS, DSH

Permissions: Configuration Read Access

Example

STUAP;

Output Format

STUAP;

```
MMI Interface Port Configuration
  USER                LOGGED_ON           LABEL
  user2               2012-03-23 10:23:12 Telnet port 8100
  siguser             2012-03-23 14:49:54 Telnet port 8101
  user2               2012-03-23 12:23:21 Web MMI
```

6.14 Command Parameters

Table 1: Command Parameters

	Dialog hunt mode. Parameter Range: CYCLIC (0) - Cyclic Selection. BALANCED (1) - Load Balanced Selection. SEQUENTIAL (2) - Sequential Selection.
AC	The application context. Parameter Range: String of length 4 to 34. Must not contain any spaces.
AC_REF	A logical identifier for this application context. Parameter Range: Number from 0 to 1023.
ACCESS	The name of an access profile that can be applied to a user giving them particular access privileges. Parameter Range: String of length 1 to 15. Must not contain any spaces.
ACTIVE	Determines whether something is active Y or inactive N. An example of its use is the activation or deactivation of trace masks (see the CNTMS command).
ADDR_FMT	Address Format. Parameter Range: PDU (0) - If configured to use ITU-T PDU formats (options bit 1 not set) use ITU-T Q.713 SCCP address format. If configured to use ANSI PDU formats (options bit 1 set) use ANSI T1.112 SCCP address format. ITU14 (1) - ITU 14-bit operation. ITU24 (2) - ITU 24-bit operation. ANSI14 (3) - ANSI 14-bit operation. ANSI24 (4) - ANSI 24-bit operation.

Table 1: Command Parameters *(Continued)*

ADDR_TYPE	The type of IP address and how it was derived. Parameter Range: STATIC_IPV4 - IPV4 Address entered through configuration. STATIC_IPV6 - Global IPV6 Address entered through configuration. LOCAL_IPV6 - Local IPV6 Address for a particular Network Interface.
AISGEN	The mode used to generate the Alarm Indication Signal (Blue alarm).
ALTMSU	ALTMSU - MSUs Sent to Alternate Peer Number of messages redirected to an alternative peer.
APC	Adjacent Point Code Parameter Range: Number between 0 to 16777215
ASC	AUTO - Automatically acknowledge AlertSC indications. This is the default value. OFF - Always reject MAN - Enable user access of AlertSC via web-service API. If this option is set user is required to retrieve AlertSC indications, if not retrieved before timeout they will be rejected
AUTH	V3 SNMP Authentication encryption protocol - used to ensure that V3 SNMP requests have not been modified during transit. Parameter Range: NONE SHA MD5
AUTHPASS	Identifies the authentication password for an SNMP User Account: The authentication protocol parameter must be present. Parameter Range: Null or Password string of length 1 to 19
AVG_PING	AVG_PING - Average Ping The average time in milliseconds the set of pings took to reach and return from the target IP node.

Table 1: Command Parameters *(Continued)*

BACKUP_HOST	The backup host algorithm. The ability to configure backup hosts allows management and/or signaling messages to be redirected to a backup host application in the event of primary host failure. When using ISUP, for example, this mechanism allows continued use of circuits if the primary host for a circuit group were to fail. Once the primary host link has been recovered, messages are again sent to it from the SIU. Backup hosts can be employed when configured for ISUP. Backup hosts may also be used for SCCP operation, they may not be used in configurations that utilize DTS/DTC. Both primary and backup hosts are configured and active. Parameter Range: BACKUP_NONE (0) - When this parameter is set to BACKUP_NONE(0) or the SIU_HOSTS command is not present, the system does not employ the backup host mechanism. BACKUP_1 (1) - When set to a BACKUP_1 (1), primary and backup hosts are paired 0-1, 2-3, 4-5 etc. If the link to host 0 fails messages are sent instead to host 1 and vice versa. When the link recovers, normal routing resumes. BACKUP_32 (2) - When set to a BACKUP_32(2), primary and backup hosts are paired 0-32, 1-33, 2-34 etc. If the link to host 0 fails messages are sent instead to host 32 and vice versa. When the link recovers, normal routing resumes.
BAK_DUAL	Use Backup route via Dual SIU.
BASE_IDLG	The base incoming dialog id. Normally expressed as a hexadecimal value. Parameter Range: Hex number from 0 to fffff
BASE_ODLG	The base outgoing dialog id. Normally expressed as a hexidecimal value. Parameter Range: Hex number from 0 to fffff
BCIC	The Circuit Identification Code (CIC) that is allocated to the first circuit in the circuit group. Parameter Range: Number between 0 to 65535
BCID	The logical ID for the first circuit in the circuit group. It must lie in the range 0 to one less than the number of circuits supported. Parameter Range: Number between 0 to 65535
BEST_PING	The time in milliseconds the best ping took to reach and return from the target IP node.

Table 1: Command Parameters *(Continued)*

BIND	Identifier to Bind a Local Application Server to either Remote. Signaling Gateway or Remote Application Server. Parameter Range: Number between 0 to 255
BLINK	The index of the logical signaling processor (SP) channel (on the board) allocated for this signaling link. When the SS7 link is to be conveyed over M2PA, the blink parameter identifies the SIGTRAN link. Parameter Range: Number between 0 to 255
BOND	The Bond Network Interface to be used. Parameter Range: NONE BOND0 BOND1 BOND2 BOND3
BPOS	Board position. Parameter Range: Number between 0 to 1
BPOS2	The board the PCM is on. Parameter Range: Number between 0 to 1
BRDTYPE	Board Type. Parameter Range: NONE SS7LD SS7MD
BUILDOUT	Specifies the range of build out settings for a T1 interface. Parameter Range: Number between 0 to 12
C7RT	SS7 Route ID. Parameter Range: Number between 0 to 4095
CAUSE	The probable cause of the alarm based on the principles of ITU Recommendations M.3100, X.733, and X.736 and GSM 12.10 (ETS 300 618).

Table 1: Command Parameters *(Continued)*

CELLSTR	An ATM Cell Stream identifier Parameter Range: Number between 0 to 7
CFGTYPE	Configuration type. Parameter Range: DEFAULT LOOPBACK
CIC_MASK	Each circuit group may contain up to 32 circuits. The CIC Mask identifies the circuits allocated to the circuit group. The least significant bit (bit 0) corresponds to the first CIC and must always be set. Bit n in the corresponds to circuit identification code = (+ n) and circuit identifier = (+ n). If the bit is not set, then this CIC and CID can instead be allocated to a different circuit group. Parameter Range: Hex number between 0 to ffffffff
CLA	Alarm class. When present the value in brackets represents the equivalent ITU-T severity level state. Parameter Range: MNR (5) - Minor alarm. MAJ (4) - Major alarm. CRT (3) - Critical alarm.
CLEARED	The date and time the alarm cleared.
CLI	Whether (Y)) or not (N) the user has MML command line interface access.
CMD	MMI command name. Parameter Range: Case sensitive string of length 5 to 5. Must not contain any spaces.
CODE	Numeric identifier of the alarm code.
CONFIGURATION ERROR	A description of a configuration error occurring on startup.
CONFIRM	Confirmation of the PASSWORD typed for remote access to MMI sessions. Parameter Range: Password string of length 1 to 79

Table 1: Command Parameters *(Continued)*

CONTACT	Designated contact for the System. Parameter Range: Null or Text of length 0 to 31. May contain spaces. '+' chars will be converted to spaces.
CRC_MODE	The Cyclic Redundancy Check (CRC) mode of operation. If displayed, the value in brackets represents the alternative integer value that can be used when entering the CRC mode during configuration of the PCM. Parameter Range: NONE (1) - CRC generation disabled. CRC4 (2) - CRC4 enabled - The frame format must be set to CRC4. CRC6 (4) - CRC6 enabled - The frame format must be set to ESF.
CRITICAL	The number of critical alarms.
CSPC	The Concerned Signaling Point Code Parameter Range: Number between 0 to 16777215
CSSN	A Remote Concerned Sub-system Number Parameter Range: Number between 0 to 254
CSSR	SCCP concerned subsystem resource type. Parameter Range: RSP - Remote signaling point. LSS - Local subsystem.
CSSRID	Concerned Subsystem Resource Identifier. Parameter Range: Number between 0 to 2047
CSSRLID	Concerned Subsystem List Identifier. Parameter Range: Number between 0 to 32767
CWND	The current congestion window for the peer address.
DATE	Calendar date. Parameter Range: Date in the form xxxx-yy-zz where xxxx is years (1990-2037), yy is months (1-12) and zz is days (1-31)
DBSVCNAME	The Database Service ID.

Table 1: Command Parameters *(Continued)*

DBSVCTYPE	The service name for the database. Note: May only be null if the service type is NONE.
DBx	Identity of the host used for connectivity to the database. Each host is identified in a compound parameter of the form x-y, where x is the Host ID and y is set to either PRI or SEC to determine the intended usage of the host. The parameter can also be set to NONE to remove a host from a service. When used as part of the status command, the y parameter will indicate FAILED when the service has lost communication with the database.
DEFVCI	A default AAL5 link will be configured for the cell stream to signal incoming active connections. This is the VCI that will be used for this connection. Values 0, 3 and 4 are reserved and should not be used. Parameter Range: Number between 0 to 65535
DEFVPI	A default AAL5 link will be configured for the cell stream to signal incoming active connections. This is the VPI that will be used for this connection. Parameter Range: Number between 0 to 65535
DEV_PING	The standard deviation of the time in milliseconds the pings took to reach and return from each the target IP node.

Table 1: Command Parameters *(Continued)*

DFDCS	Default Data Coding Scheme. Parameter Range: German English Italian French Spanish Dutch Swedish Danish Portuguese Finnish Norwegian Greek Turkish Hungarian Polish Undefined GSM_7bit - GSM 7 bit alphabet; preceded by language indication. UCS2 - UCS2; message preceded by language indication. Czech Hebrew Arabic Russian Icelandic
DFLT_ENGINE	A hexadecimal string value used to display the default engine ID for SNMP V3 traps.
DIAG1	Diagnostic associated with an alarm event. The meaning of the diagnostic field depends on the alarm type.
DIAG2	Diagnostic associated with an alarm event. The meaning of the diagnostic field depends on the alarm type.
DLGGID	The unique logical identifier of the dialog group. Parameter Range: Number from 0 to 31
DLGID	A logical identifier for a TCAP dialog, The valid range is 0 to 65535. Parameter Range: Number between 0 to 65535
DMHOST	The default management host. Parameter Range: Number between 0 to 127

Table 1: Command Parameters *(Continued)*

DPC	Destination Point Code. Parameter Range: Number between 0 to 16777215
DRIVE	A Drive bay identifier for a disk drive. Parameter Range: Number between 0 to 1
DSE	Defines whether the DSE interface is active.
DSMIEVENT	Option to select the type of traps provided by the system: OBJECT - report object-based SNMP notifications only. ALARM - report alarm-based SNMP notifications only. ALL - report both object based and alarm-based SNMP notifications. NONE - do not provide any notifications.
DSTNP	Destination Numbering Plan Parameter Range: Unknown ISDN Reserved2 Data Telex ServiceCentreSpecific5 ServiceCentreSpecific6 Reserved7 National Private ERMES Reserved11 Reserved12 Reserved13 Reserved14 Reserved

Table 1: Command Parameters *(Continued)*

DSTTON	Destination Type Of Number Parameter Range: Unknown International National NetworkSpecific Subscriber Alphanumeric AbbreviatedNumber Reserved
DTYPE	Data type. Parameter Range: SYSKEY SYSCFG CONFIG
END	Identifies whether the SIU end is acting as a client or a server. Parameter Range: C - Client Side. S - Server Side.
ENGINE	A hexadecimal string value used for a SNMP V3 engine associated with a particular manager.
ETH	Ethernet port number. Parameter Range: Number between 0 to 31
EXP	Whether the password in the account should expire (Y) or Not (N).
FE_REF	Logical identifier for this Functional Entity (FE).
FF	The Frame Format. If displayed, the value in brackets represents the alternative integer value that can be used when entering the Frame Format during configuration of the PCM. Parameter Range: G704 (1) - E1 double frame (E1 only). CRC4 (2) - E1 CRC4 multiframe (E1 only). F4 (3) - F4 4-frame multiframe (T1 only). D3D4 (4) - D3/D4 (Yellow alarm = bit 2 in each channel (T1 only). ESF (7) - ESF (Yellow alarm in data link channel) (T1 only). SLC96 (8) - F72/SLC96 (72-frame multiframe) (T1 only). J1 (9) - J1 frame format (The LIU type must be T1).

Table 1: Command Parameters *(Continued)*

FTP	Whether (Y)) or not (N) the user has FTP and Telnet over SSH access.
FTPSER	FTP Server access. Set to Y to allow access or N to disable access.
GATEWAY	Address of IP gateway. Set to 0.0.0.0 to indicate that no gateway is present. Parameter Range: IP Address of the form w.x.y.z where w,x,y and z are between 0-255
GID	The unique logical identifier of the circuit group within the SIU. This parameter is in the range 0 to one less than the maximum number of circuit groups that ISUP processes as set by the parameter in the ISUP configuration command. Parameter Range: Number between 0 to 2047
GLID	Identifier that associates a Remote Signaling Gateway with a SIGTRAN Route. Parameter Range: Number between 0 to 65279
GTAID	Identifier for a Global Title Address. Parameter Range: Number between 0 to 1023
GTPID	Identifier for a Global Title Pattern. Parameter Range: Number between 0 to 1023
GTTSRC	Identifier for the source to which the Global Title Translation applies. When GTTSRC=LOCAL the command only applies for messages generated by a local sub-system (i.e., Outgoing messages). When GTTSRC=REMOTE the command only applies to messages passed up to SCCP from the network (i.e., Incoming messages). If GTTSRC=ANY (or the parameter is omitted), the command applies to all messages.
GWADDR	Gateway Address Digits Parameter Range: Case sensitive string containing 0-9, *, #, a, b or c characters of length 1 to 30.

Table 1: Command Parameters *(Continued)*

GWNP	Gateway Numbering Plan Parameter Range: Unknown ISDN Reserved2 Data Telex ServiceCentreSpecific5 ServiceCentreSpecific6 Reserved7 National Private ERMES Reserved11 Reserved12 Reserved13 Reserved14 Reserved
GWTON	Gateway Type Of Number Parameter Range: Unknown International National NetworkSpecific Subscriber Alphanumeric AbbreviatedNumber Reserved
HDPR	Identifier of the Helix Diameter Peer.
HLRADDR	HLR Address Digits Parameter Range: Case sensitive string containing 0-9, *, #, a, b or c characters of length 1 to 30.

Table 1: Command Parameters *(Continued)*

HLRNP	HLR Numbering Plan Parameter Range: Unknown ISDN Reserved2 Data Telex ServiceCentreSpecific5 ServiceCentreSpecific6 Reserved7 National Private ERMES Reserved11 Reserved12 Reserved13 Reserved14 Reserved
HLRTON	HLR Type Of Number Parameter Range: Unknown International National NetworkSpecific Subscriber Alphanumeric AbbreviatedNumber Reserved
HOST	IP host Parameter Range: NONE (command specific) or Case sensitive string of length 1 to 47. Must not contain any spaces.
HOST	IP host. NONE or case-sensitive string length of 0 to 47. Must not contain any spaces.
HOSTID	Logical ID of an SIU host. Parameter Range: Number between 0 to 127
HOSTS	When Hosts is set the SIU does requires SIU hosts to operate. Hosts may be disabled when the SIU is acting as a router than does not require management or application hosts.

Table 1: Command Parameters *(Continued)*

HTTPPORT	The TCP Port used for HTTP. Set to 0 to disable access via HTTP. Valid Range 0:65,535 excluding 21, 22, 8100-8103, 9000-9128, the value identified by HTTPSPORT or the HTTPPORT value of another Web Server. Parameter Range: Null or Number between 0 to 65535
HTTPSCERT	Identify the certificate to use for the SERVICE. Parameter Range: NONE - The certificate for the service will be removed. SELF - A new self-signed certificate will be generated and installed. FILE - The corresponding certificate will be used.
HTTPSPORT	The TCP Port used for HTTPS. Set to 0 to disable access via HTTPS. Valid Range 0:65,535 excluding 21, 22, 8100-8103, 9000-9128, the value identified by HTTPSPORT or the HTTPSPORT value of another Web Server. Parameter Range: Number between 0 to 65535
HUNT	Destination Table Hunt type. Parameter Range: FIRST - The first available destination from the destination table will be selected starting at the lowest number row. CIRCULAR - The next available destination from the destination table will be selected in a round robin manner each time a new message is routed. BALANCE - A destination from a destination table will be selected from the Destination Table in a round robin manner on a per call basis with the next available Destination being selected each time a message matching the Routing Key contains an ISUP/BICC IAM message. The OPC, DPC and a BICC/ISUP Service indicator must be present in the routing key for IAM hunting to be used. SHARE1 - A destination from a destination table will be selected based on the SLS field in the received message. If the destination is not available the next available destination will be selected based on the SLS and the number of remaining destinations.
ID	Identifier associated with an alarm event. The meaning of the id field depends on the alarm type. Parameter Range: Number between 0 to 65535

Table 1: Command Parameters *(Continued)*

IFTYPE	The interface type for the link. Parameter Range: TDM - Single timeslot signaling link. M2PA - SIGTRAN M2PA Signaling Link. ATM - ATM Signaling Link. E1_FRAMED - Framed 31 timeslot E1 operation. T1_FRAMED - Framed 24 timeslot T1 operation. PCM - Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling)
IMALEN	The length of the IMA frame (for IMA use only). 0 - Default for non IMA operation. 1 - 32 cells per IMA frame 2 - 64 cells per IMA frame 3 - 128 cells per IMA frame 4 - 256 cells per IMA frame
IMASK	Input Mask - Trace Mask for signaling messages entering a protocol module. Parameter Range: Hex number between 0 to ffffffff
IMSI	International Mobile Subscriber Identity. Parameter Range: Case sensitive string containing 0-9, *, #, a, b or c characters of length 1 to 15.
IN_STREAM	A reference to the 2 Mbps stream for the input of a simplex connection (mode 2) or one half of a duplex cross connection (mode 3). In other modes, this field should be set to zero fixed data pattern. Parameter Range: Number from 0 to 3
INHIBIT	Inhibit action. Set to Y to inhibit an SS7 link, set to N to uninhibit the link.
IP4ADDR	An IPV4 address and subnet are expressed in CIDR notation where the IP address and subnet are separated by the \'/\' character. The subnet parameter is expressed as an integer indicating the leading (i.e., significant) 1 bits that identify the sub-net mask. For an IPv4 address this value may be up to a value of 31. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address.

Table 1: Command Parameters *(Continued)*

IP6ADDR	A IPV6 address and subnet expressed in CIDR notation where the IP address and subnet are separated by the \'/\' character. The subnet parameter is expressed as an integer indicating the leading (i.e., significant) 1 bits that identify the sub-net mask. For an IPv6 address the value can be up to 127 however common use for IPv6 is that this value is 64 to indicate that the top 64 bits of the IP address indicates the subnet the IP address exists within and the bottom 64 bits identifies the server within the subnet. Parameter Range: Null or IP address entered as one of the following:| An IPV6 Address.
IPACT	The action to be performed when the data matches the rule. Parameter Range: ACCEPT - Data will be accepted. DROP - Data will be discarded.
IPADDR	An IP Address An IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
IPDEST	A destination IP address or network identifier. Parameter Range: Null or ANY (command specific) or IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
IPFW	A logical reference for and entry in the IP Firewall list. DEFAULT is the default rule applied when other criteria are not met. Parameter Range: DEFAULT or Number between 1 to 31
IPGW	A logical reference for an Internet Protocol Gateway. DEFAULT is the default IP Gateway. Parameter Range: DEFAULT or Number between 1 to 31

Table 1: Command Parameters *(Continued)*

IPHOST_NAME	A name that is used in system configuration to represent a IPv4/ IPv6 address. Parameter Range: Null or String of length 0 to 80. Must not contain any spaces.
IPLG	A logical reference for and entry in the IP Log filter list. DEFAULT is the default rule and the other rules are applied on top of the default rule. Note: The default rule cannot be deleted, only its action modified Parameter Range: Number between 1 to 4
IPNW	An IP network identifier. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address. An IPV6 Address. May be set to DEFAULT.
IPNW	An IP network identifier. Parameter Range: Null or IP Address of the form w.x.y.z where w,x,y and z are between 0-255
IPSRC	A source IP address or network identifier. Parameter Range: Null or ANY (command specific) or IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
IPSVC	System IP Server Ports Parameter Range: Null or ALL TELNET - Telnet MML Server ports. SSH - SSH Server port. FTP - FTP Server port. WMGMT - Web Management Server ports. WSAPI - Web Server API ports. REMOTE - Port communicating with the Remote System. HOST - Ports communicating with hosts applications. SCTP - SCTP Ports. SNMP - Ports used by SNMP.

Table 1: Command Parameters *(Continued)*

IPTOKEN	A short name that is used in system configuration to represent a IPv4/IPv6 addresses. Parameter Range: String of length 1 to 16. Must not contain any spaces.
L2ID	The Layer 2 ID of the Cell Stream within the board. Parameter Range: Number between 0 to 7
LABEL	Text label used to identify the related item. Parameter Range: Null or Text of length 0 to 31. May contain spaces. '+' chars will be converted to spaces.
LANG	Language indication string. Parameter Range: Case sensitive string of length 0 to 2. Must not contain any spaces.
LAS	The SIGTRAN Local Application Server identifier. Parameter Range: Number between 0 to 255
LAST_PING	The time in milliseconds the last ping took to reach and return from the target IP node.
LC	Line Coding Technique. If displayed, the value in brackets represents the alternative integer value that can be used when entering the Line Code during configuration of the PCM. Parameter Range: HDB3 (1) - HDB3 (E1 only). AMI (2) - AMI with no Zero Code Suppression. B8ZS (4) - B8ZS (T1 only).
LEDID	Front panel LED ID. Set to Y to activate LED, or N to deactivate LED.
LGDATA	Data associated with a logging filter. The data entered is specific to the filter. Parameter Range: Null or Case sensitive string of length 0 to 31. Must not contain any spaces.

Table 1: Command Parameters *(Continued)*

LGTYPE	Logging Filter. Parameter Range: IPADDR - Outputs IP traffic associated with a configured IP Addresses. Note: Data associated with the management interfaces will not be logged. SCTP - Outputs SCTP traffic. If specified, the associated data can be used to limit the output to the particular local SCTP port which would normally be a local port associated with a SIGTRAN link. HOST - Outputs traffic send and received from RSI Hosts. If specified, the associated data can be used to limit the output to RSI host id. REMOTE - Outputs traffic send and received from a Partner Server. The associated data field must be blank. UDP - Outputs UDP (SNMP) traffic. If specified, the associated data can be used to limit the output to the particular local UDP port. WSAPI - Outputs traffic send and received from Web Service Hosts. The associated data field must be blank.
LINE	For Telnet and Serial MMI the number of lines that may be displayed before being prompted to continue. A value of 0 indicates that commands will output to completion without further prompting. The parameter is not applicable for Web management MMI. Parameter Range: Number from 0 to 100
LINK	SS7 link identifier. Parameter Range: Number between 0 to 255
LINKSET	Link Set ID. Parameter Range: Number between 0 to 63
LIP1	The first Local IP Address. Parameter Range: An IP address entered as one of the following: An IPV4 Address. A 15 character IPTOKEN string configured to map to an IP Address.

Table 1: Command Parameters *(Continued)*

LIP2	The second Local IP Address. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address. A 15 character IPTOKEN string configured to map to an IP Address.
LIUTYPE	Specifies the physical type of interface required. If displayed, the value in brackets represents the alternative integer value that can be used when entering the LIU type during configuration of the PCM. Note: Use of the Buildout parameter is not relevant when high impedance is configured on a PCM. Users are required to set it to a value of 0 for when either E1 high-impedance or T1 high impedance is configured on the PCM. Parameter Range: T1 (4) - T1. E1 (5) - E1 balanced. E1HIGHZ (6) - E1 high-impedance (for monitoring applications). T1HIGHZ (7) - T1 high-impedance (for monitoring applications). E1PMP (8) - E1 protective monitoring point (for monitoring applications). T1PMP (9) - T1 protective monitoring point (for monitoring applications).
LOCAL_IPADDR	Local IP address. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
LOCATION	The location of this System. Parameter Range: Null or Text of length 0 to 31. May contain spaces. '+' chars will be converted to spaces.
LOGLVL	Flow environment debug log level. Number from 0 to 6.
LOOPMD	The diagnostic loopback mode.
LOSS_PCT	The percentage of packets lost.
LPORT	Local IP port for an association. Parameter Range: Number between 0 to 65535
LS1	The first Link Set on a Route. Parameter Range: Number between 0 to 63

Table 1: Command Parameters *(Continued)*

LS2	The second Link Set on a Route Parameter Range: Number between 0 to 63
LSSPROT	Local Subsystem Protocol. Parameter Range: SCCP - The SCCP protocol. TCAP - The TCAP protocol. MAP - The MAP protocol. INAP - The INAP protocol. IS41 - The IS41 protocol. DTS - DTS running over the SCCP protocol. DTS_MAP - DTS running over the MAP protocol. DTS_INAP - DTS running over the INAP protocol. DTS_IS41 - DTS running over the IS41 protocol.
M2PAID	M2PA Identifier. Parameter Range: Number between 0 to 255
M3UASHARE	Only required to be set to a non blank value when both M3UA and network facing M2PA links are configured at the same time. This parameter is percentage share of the SIGTRAN portion of server license allocated to M3UA links with the remaining percentage being available for network facing M2PA links. The SIGTRAN portion of the server license is determined by the value of the TDM Share parameter. Values are blank or 1-99. When set to blank the full allocation of the server license is available to either M3UA or Network facing M2PA links however in this case both may not be configured at the same time. Parameter Range: Null or Number between 1 to 99
MAJOR	The number of major alarms.

Table 1: Command Parameters *(Continued)*

MAP_SERVICE	The MAP Web Service. Parameter Range: Mobile_Term_Transmit_Reqs - SMS Mobile Terminated Transmit Requests. Mobile_Term_Receive_Reqs - SMS Mobile Terminated Receive Requests. USSD_Mobile_Init_Sessions - USSD Mobile Init Sessions. USSD_App_Init_Sessions - USSD App Init Sessions. USSD_Notify_Reqs - LBS Location Requests. Location_Service_Reqs - USSD Notify Requests. Mobile_Orig_Transmit_Reqs - SMS Mobile Originated Transmit Requests. Mobile_Orig_Receive_Reqs - SMS Mobile Originated Receive Requests.
MASK	An IP network mask. Parameter Range: Null or IP Address of the form w.x.y.z where w,x,y and z are between 0-255
MAXLIFE	The maximum number of days allowed before a new password must be entered. Parameter Range: Null or Number between 1 to 600
MAXSIF	Specifies the maximum size of a message transmitted. For ISUP operation, this should be 272 octets. For BICC operating above M3UA, a user may specify up to 544 octets to allow larger messages to be transmitted without the need for segmentation. Support for sif values above 272 is application dependant and depends on the maximum size a receiving switch can process. Parameter Range: Number from 272 to 4200
MGA	Whether (Y)) or not (N) the user has administrative management access to add/remove users.
MGMT	Management web interface availability. Set to Y to enable Management web interface on a particular IP address. Set to N to disable Management web interface on a particular IP address.
MGP	Whether (Y)) or not (N) the user has policy access to set system policy.
MGR	Whether (Y)) or not (N) the user has access to read configuration, status and measurements.
MGS	Whether (Y)) or not (N) the user has access permission to modify security settings such as the system firewall.

Table 1: Command Parameters *(Continued)*

MGW	Whether (Y)) or not (N) the user has access permission to Change/Add/Delete configuration.
MGX	Whether (Y)) or not (N) the user has access permission to perform maintenance actions (activate/deactivate/restart)
MHOST	A * indicates that a host is acting as a management host.
MIN_HOSTS	The minimum number of hosts required before Network Side SIGTRAN or TDM links enter service.
MINOR	The number of minor alarms.
MLINK	SS7 Monitor link identifier. Parameter Range: Number between 0 to 255
MMASK	Management Mask - Trace Mask for management messages generated by a protocol module. Parameter Range: Hex number between 0 to ffffffff
MMIPORT	MMI Port Identifier Parameter Range: Number between 0 to 4
MNGR	A logical reference for an External SNMP Manager Parameter Range: Number between 1 to 31
MNGR_IPADDR	SNMP Manager IP address. Parameter Range: An IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
MNGT_HOST	The Host ID for management messages. Parameter Range: Number from 0 to 127
MNID	The Node ID for nodes within a Multi-Node cluster.

Table 1: Command Parameters *(Continued)*

MNMODE	The mode of operation for a Node within a Multi-Node cluster. The parameter takes the following values: STANDALONE - System operating as a Standalone Node. MASTER - System operating as a Master of Mutli-Node Cluster. SEC_MASTER - System operating as a Secondary Master of a Multi-Node Cluster. GROUP_MEMBER - System operating as a Group Member of Multi-Node Cluster.
MODE	This parameter is used to select the operating mode of the unit. A unit that is operating as a standalone unit should be operated in A mode. When two units are used in a dual resilient configuration, one unit should operate in A mode and the other should operate in B mode. Changes to the parameter value require a system restart in order to take effect. Parameter Range: MODEA - System operating in A Mode. MODEB - System operating in B Mode.
MODULE	Protocol module name. Parameter Range: MTP M3UA ISUP SCCP DTS TCAP IS41 INAP MAP MSL WSI

Table 1: Command Parameters *(Continued)*

MTP2_TIM_TBL	MTP2 Timer table. Parameter Range: ALL (8) - Setting applies to all MTP2 timer tables. ITU (0) - Setting only applies to the MTP2 ITU-T 64k link timer table. ANSI64K (1) - Setting only applies to the MTP2 ANSI 64k link timer table. ANSI56K (2) - Setting only applies to the MTP2 ANSI 56k link timer table. ITU48K (3) - Setting only applies to the MTP2 ITU-T 48k link timer table. ANSIT1 (4) - Setting only applies to the MTP2 ANSI T1 link timer table. ANSIE1 (5) - Setting only applies to the MTP2 ANSI E1 link timer table. ITUT1 (6) - Setting only applies to the MTP2 ITU-T T1 link timer table. ITUE1 (7) - Setting only applies to the MTP2 ITU-T E1 link timer table.
MWS	Whether (Y)) or not (N) the user has Management web server access.
NA	Network Appearance. Parameter Range: Number between 0 to 4294967295
NASP	The number of ASP (SIGTRAN Links) required in load sharing mode. Parameter Range: Number between 0 to 256
NC	Network context NC0 to NC3. If not specified default NC is considered which is NC0. Parameter Range: NC0 - Network Context 0. NC1 - Network Context 1. NC2 - Network Context 2. NC3 - Network Context 3.

Table 1: Command Parameters *(Continued)*

NETIF	The Network Interface. Note: Ethernet Network Interfaces cannot be added or removed from the configuration. Parameter Range: ETH0 ETH1 ETH2 ETH3 ETH4 ETH5 ETH6 ETH7 BOND0 BOND1 BOND2 BOND3
NLINKS	The (maximum) number of links allocated to the link set. Parameter Range: Number between 1 to 16
NODE	User assigned short form system identity. Null or Case sensitive string containing a-z, A-Z or 0-9 characters of length 0 to 9.
NODENAME	IP node name. Parameter Range: Case sensitive string of length 1 to 47. Must not contain any spaces.
NR1D	Peak rate of MSUs received during the last day (msu/s)
NR1H	Peak rate of MSUs received during the last hour (msu/s)
NR5M	Peak rate of MSUs received during the last 5 minutes (msu/s)
NSUBP	Y - Use Version 1 Map operation Note Subscriber Present, if set. N - Use Version 2 Map operation MAP Ready For SM, if set (default).
NT1D	Peak rate of MSUs transmitted during the last day (msu/s)
NT1H	Peak rate of MSUs transmitted during the last hour (msu/s)
NT5M	Peak rate of MSUs transmitted during the last 5 minutes (msu/s)
NTP	NTP activation parameter. Set to Y to enable use of Network Time Protocol or N to disable use of Network Time Protocol.
NTPSER	Identifier for the NTP server Parameter Range: Number between 0 to 15

Table 1: Command Parameters *(Continued)*

NTPSER_IPADDR	NTP Server IP address. Parameter Range: An IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
NUM_CCTS	Number of circuits allowed. Parameter Range: Number from 1 to 65535
NUM_CGRPS	Number of circuit groups allowed. Parameter Range: Number from 1 to 2048
NUM_DPCS	The number of Destination Point Codes. Parameter Range: Number from 0 to 32
NUM_HOSTS	Number of hosts allowed. Parameter Range: ALL (command specific) or NONE (command specific) or Number from 0 to 128
NUM_IDLG	The number of incoming dialogs. Parameter Range: Hex number from 0 to 100000
NUM_ODLG	The number of outgoing dialogs. Parameter Range: Hex number from 0 to 100000
OBJECT	A logical reference for an SNMP object within an object group: Parameter Range: Number between 0 to 65535
OBJGRP	A logical reference for an SNMP object group: Parameter Range: Number between 0 to 65535
OBJIDX	An index used as a unique reference to a SNMP object which is constructed by multiplying the object group by 100 an then adding the object within the group.
OCCURRED	The date and time the alarm occurred.

Table 1: Command Parameters *(Continued)*

OFFSET	The local offset from UTC in Hours and Minutes. Hours may be specified in the range -14 to +12, and minutes in either 0 or 30 minute intervals. The offset is specified in POSIX-style, which has positive signs west of Greenwich. e.g. Montreal, CANADA +5:00 USA +5:00 UNITED KINGDOM 0:00 GERMANY -1:00 New Delhi, INDIA -5:30 Beijing, CHINA -8:00 Sydney, AUSTRALIA -10:00 Parameter Range: Case sensitive string of length 0 to 9. Must not contain any spaces.
OMASK	Output Mask - Trace Mask for signaling messages leaving a protocol module. Parameter Range: Hex number between 0 to ffffffff
OPC	The originating point code. Parameter Range: Number between 0 to 16777215
OPTIONS	Configuration Options. Parameter Range: Null or Hex number between 0 to ffffffff
OPTIONS2	Additional Configuration Options. Parameter Range: Null or Hex number between 0 to ffffffff
OR1D	Percentage 1 day peak link receive utilization in a 10s period
OR1H	Percentage 1 hour peak link receive utilization in a 10s period
OR5M	Percentage 5 minutes peak link receive utilization in a 10s period
ORGADDR	Originating Address digits Parameter Range: Case sensitive string containing 7 BIT ASCII characters of length 1 to 30. Must not contain any spaces.

Table 1: Command Parameters *(Continued)*

ORGNP	Originating Numbering Plan Parameter Range: Unknown ISDN Reserved2 Data Telex ServiceCentreSpecific5 ServiceCentreSpecific6 Reserved7 National Private ERMES Reserved11 Reserved12 Reserved13 Reserved14 Reserved
ORGTON	Originating Type Of Number Parameter Range: Unknown International National NetworkSpecific Subscriber Alphanumeric AbbreviatedNumber Reserved
OT1D	Percentage 1 day peak link transmit utilization in a 10s period
OT1H	Percentage 1 hour peak link transmit utilization in a 10s period
OT5M	Percentage 5 minutes peak link transmit utilization in a 10s period
OUT_STREAM	A reference to the 2 Mbps stream for the output of the connection or the fixed data pattern. Parameter Range: Number from 0 to 3
OUTPUT_PATTERN	One byte of fixed data to output in pattern mode on the output stream/timeslot. Parameter Range: Hex number from 0 to ff

Table 1: Command Parameters *(Continued)*

PAGE	Selects the specific page to display for the command. Parameter Range: Number between 1 to 10
PASSWORD	Password to access to a particular account Parameter Range: Password string of length 1 to 79
PCMASK	A 32-bit value that specifies the part of a destination point code that must match the remote SPC value in order for an SCCP transmit message to be sent down to this destination sub-system. Bits set to zero indicate that the corresponding bit position in the transmit message destination point code must match the bit position of the remote SPC. Bits set to 1 indicate bit positions in the message destination point code that do not need to match the remote SPC set for this RSP. This allows configuration of a default destination sub-system (for example, a gateway SCP). Parameter Range: Hex number between 0 to ffffffff
PING_IPADDR	IP address to ping. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
PMTU	The current Path MTU for the peer address. This is the number of bytes available in an SCTP packet for chunks.
POOL	The grouping identifier for a group of items.
PORTID	PCM Port ID. Parameter Range: Number between 0 to 7
PRBSGEN	The diagnostic loopback mode.
PRIV	Identifies the privacy protocol for an SNMP User Account: Parameter Range: Null or NONE DES AES
PRIVPASS	Identifies the privacy password for an SNMP User Account: The privacy protocol parameter must be present. Parameter Range: Null or Password string of length 1 to 19

Table 1: Command Parameters *(Continued)*

PTMODE	Type of MMI Port Parameter Range: NONE - Serial port without DTR/DSR active. DTRDSR - Serial port with DTR/DSR active. TELNET - Telnet port. WEB - Web management interface.
QCUR	Current message queue size.
QMAX	Maximum message queue size during the measurement period.
RANGE	The range parameter. An example of its use is specifying a range of TCAP dialogs to be displayed by the STTDP command. Parameter Range: Number between 0 to 65535
RAS	The SIGTRAN Remote Application Server identifier. Parameter Range: Number between 0 to 255
RC	Routing Context Parameter Range: Number between 0 to 4294967295
RCOM	SNMP read-only community string Parameter Range: Null or String of length 0 to 12. Must not contain any spaces.
RCOPT	Request reception of optional parameters.
RDEL	Y - Automatically send ReportSMDelivery update indication to HLR. These updates are only generated for Web-Service API request via the combined SMS delivery requests addressed using the MSISDN. Users of the separate SendRoutingInfo and ForwardSM request API calls can generate the ReportSMDelivery indications manually using an API call. N - No not automatically send ReportSMDelivery. This is the default value.
REALM	IP realm name. NONE or case-sensitive string length of 0 to 47. Must not contain any spaces.

Table 1: Command Parameters *(Continued)*

RECOVERY	The recovery mechanism to use should a database lookup fail. Possible values are: CONTINUE - continue by forwarding the message to the original called address. RETURN - based on the Return on Error flag in the message, either return the message to the originator as a UDTS or discard the message. DISCARD - discard the message.
REF	The logical identity of the signaling link within the link set. Parameter Range: Number between 0 to 15
REMOTE_IPADDR	The IP address of the partner System in a dual resilient configuration. Parameter Range: Null or IP address entered as one of the following: An IPV4 Address. An IPV6 Address.
RESERVED	This field is reserved and should be set to 0. Parameter Range: Number between 0 to 0
RESERVED1	This field is reserved and should be set to 0. Parameter Range: Number between 0 to 0
RESERVED2	This field is reserved and should be set to 0. Parameter Range: Number between 0 to 0
RESET	Performs a reset operation when set to Y.

Table 1: Command Parameters *(Continued)*

RESTART	Restart mode. Parameter Range: SOFT - The system will restart the System application software. SOFT resets may be used for a more rapid system restart after updating system configuration. PREVIOUS - The system will restart the application software, reverting to the previous version of the software distribution if available. Note: If a software distribution for a different mode of operation has been loaded, then the system will not unable to revert to a previous version of any distribution type. EVALUATION - The system will be restarted in 1 hour evaluation mode with all licensable capabilities available for use. HALT - The system will shut down without a subsequent restart.
RETRIES	The maximum number of database retries to attempt before declaring failure.
RIID	Routing Indicator ID. This is a number from 0 to 65535.
RIP1	The first SCTP Remote IP Address in the association. Parameter Range: An IP address entered as one of the following: An IPV4 Address. A 15 character IPTOKEN string configured to map to an IP Address.
RIP2	The second SCTP Remote IP Address in the association. Parameter Range: Null or an IP address entered as one of the following: An IPV4 Address. A 15 character IPTOKEN string configured to map to an IP Address.
RLID	Identifier that associates a RAS with a SIGTRAN Link. Parameter Range: Number between 0 to 8191
RPFILTER	Reverse the path filter to protect against packet spoofing by disabling the ability to respond to asymmetrically routed packets. When set to 0, the filter is disabled. When set to 1, validation is performed by the reversed path, as specified in RFC1812.
RPORT	Remote IP port for an association. Parameter Range: Number between 0 to 65535

Table 1: Command Parameters *(Continued)*

RSG	The SIGTRAN Remote Signaling Gateway identifier. Parameter Range: Number between 0 to 255
SCADDR	Service Center Address Digits Parameter Range: Case sensitive string containing 0-9, *, #, a, b or c characters of length 1 to 30.
SCCP_ADDR	SCCP Address. Parameter Range: String of length 4 to 20. Must not contain any spaces.
SCNP	Service Center Numbering Plan Parameter Range: Unknown ISDN Reserved2 Data Telex ServiceCentreSpecific5 ServiceCentreSpecific6 Reserved7 National Private ERMES Reserved11 Reserved12 Reserved13 Reserved14 Reserved
SCTON	Service Center Type Of Number Parameter Range: Unknown International National NetworkSpecific Subscriber Alphanumeric AbbreviatedNumber Reserved
SCTP	SCTP availability. Set to Y to enable SCTP operation on a particular IP port. Set to N to disable SCTP operation on a particular IP port.
SEC_GTAID	ID of secondary translation address.

Table 1: Command Parameters *(Continued)*

SEQUENCE	Sequential reference number of an entry in the alarm log.
SESSIONS	Access Management of user logon sessions. Parameter Range: STATIC_TAGS - When selected this option disables rotating sessions tags which provide additional security by requiring transmitted URLs to use a unique key provided by the server (i.e., data and actions can only be accessed/performed by selecting operations on the web page and copying URLs), using browser refresh or forward/back buttons will not work. When using this option to ensure a secure environment is recommended that HTTPS only management access be employed requiring users to enter a password before being granted access to the server. ROTATING_TAGS - When selected this option enables rotating sessions tags which provide additional security by requiring transmitted URLs to use a unique key provided by the server (i.e., data and actions can only be accessed/performed by selecting operations on the web page and copying URLs), using browser refresh or forward/back buttons will not work. Only one user may access the server when this option is selected.
SEVERITY	The perceived severity of the active alarm: CLR (1) - cleared alarm. IND (2) - indeterminate alarm. CRT (3) - critical alarm. MAJ (4) - major alarm. MNR (5) - minor alarm. WRN (6) - warning alarm.
SHARE	The percentage share of a license that is available to a capability. For SIGTRAN capabilities this is a percentage of the throughput. For the TDM capability this is the percentage of links available. The share is controlled using the TDM share and M3UA share parameters on the system configuration command. If the share is less than the configured values of the appropriate TDM or M3UA share then another license, e.g. a system license or the specific configuration of a resource e.g. a TDM link, has resulted in a reduction the of share available to the license. Blank means not applicable. Parameter Range: Null or Number between 0 to 100

Table 1: Command Parameters *(Continued)*

SI	The Service Indicator. If displayed, the value in brackets represents the alternative integer value that can be used when entering the Service Indicator during configuration. Parameter Range: SCCP (3) ISUP (5) BICC (13) RESERVED4 (4) RESERVED6 (6) RESERVED7 (7) RESERVED8 (8) RESERVED9 (9) RESERVED10 (10) RESERVED11 (11) RESERVED12 (12) RESERVED14 (14) RESERVED15 (15)
SLAVE	Identifies an optional slave port where alarm conditions occurring on the LIU will be mapped to AIS on the slave port. Parameter Range: Number between 0 to 7
SLC	The signaling link code for a signaling link. Parameter Range: Number between 0 to 15
SNLINK	SIGTRAN link identifier. Parameter Range: Number between 0 to 255
SNMP	SNMP active parameter. Set to Y to enable operation of SNMP or N to disable operation of SNMP.
SNMPUSER	An integer identifier for a SNMP User. Parameter Range: Null or Number between 1 to 31
SNRT	The SIGTRAN route identifier. Parameter Range: Number between 0 to 255

Table 1: Command Parameters *(Continued)*

SNTYPE	Type of SIGTRAN link Parameter Range: M3UA M2PA
SPC	Signaling Point Code Parameter Range: Number between 0 to 16777215
SPEED	The speed of the Ethernet port in MHz. H indicates Half-Duplex otherwise it is Full-Duplex) Parameter Range: AUTO 10 100 1000 10H 100H
SRTT	The current calculated smoothed round-trip time for the peer address in milliseconds
SS7MODE	SS7 Mode. Parameter Range: ITU14 - ITU 14-bit operation. ANSI - ANSI 24-bit operation. ITU24 - ITU 24-bit operation. ITU16 - ITU 16-bit operation.
SSF	The value to be used in the sub-service field of level 3 messages for this link set. Parameter Range: Hex number between 0 to f
SSHSER	SSH/SFTP Server access. Set to Y to allow access or N to disable access.
SSN	SSN Subsystem number. Parameter Range: Number between 0 to 254

Table 1: Command Parameters *(Continued)*

SSR	SCCP subsystem resource type. Parameter Range: RSP - Remote signaling point. RSS - Remote subsystem. LSS - Local subsystem.
SSRID	Subsystem Resource Identifier. Parameter Range: Number between 0 to 2047
STATE	The current state of the alarm: CLR - the alarm has cleared. ACK - the active alarm has been acknowledged. ACT - the alarm is active.
STREAM	The logical PCM highway from which the signaling processor is to insert the signaling. Parameter Range: Number between 0 to 3
STRONG	When set strong passwords are required. A strong password must: - Be between 8 and 15 characters in length. - Passwords must contain at least one upper case character, one lower case character, one digit and one special character (~ $ % ^ @ #) - Must not be the same as any of the previous 8 passwords.
SUBNET	IP sub-net mask. Parameter Range: IP Address of the form w.x.y.z where w,x,y and z are between 0-255
SYNCPRI	PCM Synchronization priority. Parameter Range: Number between 0 to 32
SYSID	User-assigned long form system identity. Null or Case sensitive text of length 0 to 31. May contain spaces. '+' chars will be converted to spaces.
SYSREF	The system reference number. Parameter Range: Number between 0 to 999

Table 1: Command Parameters *(Continued)*

SYSTYPE	The operating mode of the system. Parameter Range: TEST - Server Test Mode. SIU - Signaling Interface Unit. SWS - Signaling Web Server.
TACTIVE	The duration since the peer has been activated. 0 if this cannot be determined.
TCOM	SNMP Trap community string. Is passed in each trap to an external SNMP Manager. Parameter Range: Null or String of length 0 to 12. Must not contain any spaces.
TCONGC	Total number of transactions that failed due to queue congestion.
TDMSHARE	Only required to be set to a non blank value when both TDM and SIGTRAN links are configured at the same time. This parameter is percentage share of the server license allocated to MTP2 links with the remaining percentage being available for SIGTRAN links. Values are blank or 1-99. When set to blank the full allocation of the server license is available to either MTP2 or SIGTRAN links however in this case both may not be configured at the same time. Parameter Range: Null or Number between 1 to 99
TDOWN	SNMP Trap actions in the DOWN state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TDROP	Total number of transactions that failed during framework processing and are dropped.
TELSER	Telnet Server access. When set to SECURE the Command Line Interface can only be achieved by running Telnet/SSH.
TESTMSISDN	Test MSISDN that is present in the MNP database. Note: May only be null if the service type is NONE.
TFAIL	Total number of failed transactions.

Table 1: Command Parameters *(Continued)*

TFORMAT	The format of SNMP Traps sent to the external SNMP Manager. Parameter Range: NONE - Set when using SNMP V3. V1TRAP - SNMP Version 1 format. V2TRAP - SNMP Version 2 Notification Trap. V2INFO - SNMP Version 2 Information.
TIME	Time of day. Parameter Range: Time in the form xx:yy:zz where xx is hours (0-23), yy is minutes (0-59) and zz is seconds (0-59)
TIMID	A string identifier the specific timer. Parameter Range: String of length 0 to 14. Must not contain any spaces.
TIMPAIR	SNMP Trap actions in the IMPAIRED state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TIMTAB	The timer table. Specified as an integer.
TINACTIVE	SNMP Trap actions in the INACTIVE state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TINSTATE	The current duration that the peer has been in the present connection state. 0 if this cannot be determined.
TLO	The inactivity time in minutes before a MMI port automatically logs off.

Table 1: Command Parameters *(Continued)*

TLOW	The time inactivity before a MMI port provides a logoff warning. Parameter Range: Number from 0 to 50
TMSEC	A timer value in milliseconds.
TNOFLOW	Total number of transactions that failed due to an unknown flow determination.
TPFAIL	Total number of transactions that failed during module processing.
TPORT	SNMP destination port for SNMP Traps. Parameter Range: Number between 0 to 65535
TQUIESCE	SNMP Trap actions in the QUIESCED state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TRACEFMT	Identifies the format used for trace messages sent to file Parameter Range: TEXT - Trace messages will be logged to file in TEXT format. PCAP - Trace messages will be logged to file in PCAP format. DUAL - Trace messages will be logged to file in both PCAP and TEXT format.
TRACELOG	Identifies where trace messages should be logged Parameter Range: FILE - Trace messages will be locally logged to file but not transmitted to a management host. HOST - Trace messages will be transmitted to a management host but not locally logged to file. DUAL - Trace messages will be locally logged to file and transmitted to a management host.
TRACELVL	Flow environment debug trace level. Number from 0 to 6.
TRANS	Total number of successful transactions.

Table 1: Command Parameters *(Continued)*

TRAP	SNMP Trap actions. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TRESTART	SNMP Trap actions in the RESTART state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TRMD	The traffic mode for the Local Application Server. Parameter Range: LS - Loadshare. BC - Broadcast. OR - Override.
TS	Timeslot on a PCM. Parameter Range: Number between 0 to 31
TSEC	A timer value in seconds.
TSHUT	Total number of transactions that failed during framework shutdown and are dropped.
TSMASK	Hex number from 0 to ffffffff
TTOTAL	Total number of transactions.
TTOUT	Total number of transactions that failed due to a timeout.

Table 1: Command Parameters *(Continued)*

TUP	SNMP Trap actions in the UP state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TWARNING	SNMP Trap actions in the WARNING state. Parameter Range: ALL - Any event when the object is in this state will result in a trap. NONE - No event when the object is in this state will result in a trap. CREATE - Configuration events resulting in a transition to this state will result in a trap. CHANGE - Change events in this state will result in a trap. DESTROY - Configuration change events in this state will result in a trap.
TXTPREF	Whether the receipt of text is preferred (Y) over SMS network headers (N).
TYPE	Classification of the alarm into an alarm type from the following list: communicationsAlarm (2), qualityOfServiceAlarm (3), processingErrorAlarm (4), equipmentAlarm (5) and environmentalAlarm (6).
TZONE	The timezone. If set to UTC_Offset the UTC_OFFSET parameter will be used to set the offset time from UTC. If set to another value the local time will be set based on the city selected. If UTC_Offset is used then automatic daylight saving time adjustments are not performed. If a specific region is selected then daylight saving time adjustments will automatically be made. If a sub-region is unique across all regions then when entering the sub-region value the region need not be specified e.g. either "Europe_London" or "London" may be entered. The value showing the region will always be displayed.
UNITID	Fixed unique identifier for this unit, used for licensing.

Table 1: Command Parameters *(Continued)*

UPMASK	A 16-bit value with bit n (in the range 3 to 15) set to allow the route to be used for messages with Service Indicator (SI) n. For each user part supported, the bit corresponding to the Service Indicator for that user part should be set. For example, to enable SCCP routing (which uses an SI of 3) a value of 0x0008 should be used. To enable both SCCP (3) and ISUP (5) a value of 0x0028 should be used or to enable SCCP (3) and BICC (13) a value of 0x2008 should be used. Parameter Range: Hex number between 0 to ffff
UPMODE	Object to be updated. Parameter Range: LIU ATMC CGRP MTPR MTPLS MTPL MONL SSR CSSR SNLINK SNLAS SNRAS SNRASL SNRT SNRTL SNBIND
USER	A User Account identifier Parameter Range: String of length 2 to 19. Must not contain any spaces.
USER_HOST	The host ID of the user application. Parameter Range: Number between 0 to 127
USER_ID	The user application module ID for this circuit group. Parameter Range: Hex number between 0 to ff

Table 1: Command Parameters *(Continued)*

UTC_OFFSET	The local offset from UTC in Hours and Minutes. Hours may be specified in the range -14 to +12, and minutes in either 0 or 30 minute intervals. The offset is specified in POSIX-style, which has positive signs west of Greenwich. e.g. Montreal, CANADA +5:00 USA +5:00 UNITED KINGDOM 0:00 GERMANY -1:00 New Delhi, INDIA -5:30 Beijing, CHINA -8:00 Sydney, AUSTRALIA -10:00
VARIANT	ISUP variant. If displayed, the value in brackets represents the alternative integer value that can be used when entering the ISUP variant during configuration of the circuit group. Parameter Range: BB (0) - Blue Book ISUP. ITU92 (1) - 1992 (White Book) ISUP. ANSI (2) - ANSI ISUP. GERMAN (3) - German ISUP. UK (4) - UK ISUP. TTC (5) - Japanese TTC ISUP. ANSI_RLT (6) - ANSI Release Link Trunk ISUP. ITU_RLT (7) - ITU Release Link Trunk ISUP. ANSI_95 (8) - ANSI 95 ISUP. ITALIAN (9) - Italian ISUP. SSURF (10) - French SSURF ISUP. CHINA (11) - Chinese ISUP. ITU_2000 (12) - ISUP 2000/ETSI V4 ISUP. BICC (13) - The BICC protocol. CUSTOM1 (254) - Custom ISUP Variant 1. CUSTOM2 (253) - Custom ISUP Variant 2.
VCI	The VCI associated with the link on the cell stream. Parameter Range: Number between 0 to 65535
VPI	The VPI associated with the link on the cell stream. Parameter Range: Number between 0 to 65535
WARNING	The number of warning alarms issued.

Table 1: Command Parameters *(Continued)*

WEBSERV	Specifies the type of Web Server to configure. Parameter Range: MGMT - Web Server used for System Management. WSAPI - Web Server used for the Web Services API.
WMSER	Web Management access. Parameter Range: INACTIVE - Deactivate the web server. ACTIVE - Activate the web server. SECURE - Activate the web server requiring that access is granted only after the entry the entry of a user name and password. HTTPS - Activate the web server requiring that access is granted only after the entry of a user name and password. Also only allow operation over HTTPS.
WORST_PING	The time in milliseconds the worst ping took to reach and return from the target IP node.
WSAPI	Web Services API availability. Set to Y to enable Restful web interface on a particular IP address. Set to N to disable Restful web interface on a particular IP address.
WSS	Whether (Y)) or not (N) the user has Web Services API access.
WSSER	Web Services access. Parameter Range: INACTIVE - Deactivate the web server. ACTIVE - Activate the web server. SECURE - Activate the web server requiring that access is granted only after the entry the entry of a user name and password. HTTPS - Activate the web server requiring that access is granted only after the entry of a user name and password. Also only allow operation over HTTPS.
XCON_MODE	Cross connect mode Parameter Range: PATTERN (1) - Set a fixed pattern specified by OUTPUT_PATTERN on the output timeslot(s). SIMPLEX (2) - Connect the input timeslot to the output timeslot. DUPLEX (3) - Duplex cross-connect the input and output timeslot.

7 Configuration Guidelines

7.1 Overview

Configuration guidelines are provided for the following:

- "IP Port Bonding"
- "Sharing Licensed Throughput Between Protocols and Networks"
- "Configuring Multiple Network Contexts"
- "Configuring an ANSI System"
- "Specifying Default Routes"
- "Dynamic Host Activation"
- "Dynamic Configuration"
- "SIGTRAN M2PA Signaling"
- "Simultaneous MAP/INAP/IS41 Operations"
- "GTT Configuration"
- "HSL Signaling"
- "Monitoring"

7.2 IP Port Bonding

The Signaling Server allows you to configure a resilient IP connection across an IP port bonding team of two ports in an active/standby configuration. On the Dialogic® DSI SS7G41 Signaling Servers, up to two port bonding teams may be created using the four Ethernet ports on the SIU, described in IPNII - IP Network Interface Initiate and IPNIC - IP Network Interface Change.

If the system detects that a port has failed, it passes the MAC and Layer 3 address of that port to the failover adapter, enabling it to act as the active port in the team.

Data loss may occur between the actual failure of an IP connect and the detection of that failure and subsequent switching to the standby port.

All adapters in a team should be connected to the same hub or switch with Spanning Tree (STP) set to **off**.

Whenever bonding is activated, or deactivated, MMI sessions using those ports are reset.

Once configured, the status of Ethernet ports in a bonded team may be checked using the STNIP – Status Network Interface command.

7.3 Sharing Licensed Throughput Between Protocols and Networks

The SIU and SWS license SKUs identified in Section 2.1.2, “Supported Licenses” on page 20 identify a throughput element in terms of link equivalents. If the system is configured to use both TDM and SIGTRAN or configured to use more than one Network Context then a portion of the license must be allocated to TDM, M3UA and M2PA as applicable.

If M3UA is split across multiple Network Context, the M3UA portion of the license must further be split with a portion allocated to each Network Context.

When both TDM and SIGTRAN signaling are required on the server then the TDMSHARE parameter on the CNSYS MMI command should be specified to indicate the percentage share of the throughput aspect of the license that should be allocated to TDM signaling with the remainder being available to SIGTRAN (M3UA or network facing M2PA). If TDMSHARE is set to blank then either TDM or SIGTRAN (but not both) may be configured and the configured signaling will be allocated the full share of the license.

When both M3UA and network facing M2PA are required on the server the percentage share available to SIGTRAN can be further sub-divided between M3UA and M2PA using the M3UASHARE parameter on the CNSYS MMI command in a similar manner to TDMSHARE. If TDMSHARE is set to blank then the M3UASHARE parameter determines what portion of the full license is available to M3UA and what is available to M2PA.

Finally, if M3UA is required to operate in multiple networks, the portion of the license allocated to M3UA may further be split across those networks by using the SHARE value in each STN_CONFIG command associated with each Network Context. Cumulatively, the values of these ‘shares’ must add up to ‘100’ representing 100 percent of the licensed throughput that has been allocated to M3UA.

7.4 Configuring Multiple Network Contexts

7.4.1 Multiple Network Support

The SS7 Network Context together with a signaling point code uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. The Network Context may be a unique identifier for a physical SS7 network, for example, to identify an ANSI, ITU, International or National network, or it may be used to subdivide a physical SS7 network into logical sub-networks. An example of the use of logical networks is in provisioning, where the user requires 64 SS7 links between two point codes in a network. As the SIU supports 16 links in a link set, and one link set between two points in a network, only 16 links between two points would normally be achievable. However, if the network is divided into four logical Network Contexts, then up to four link sets may be created between the two point codes, one in each Network Context, thus allowing up to 64 SS7 links to be configured between the two points.

Note: The Network Context has significance only to the configuration of the local node (including the hosts). No external messages include any indication of the Network Context and the configuration of remote systems is unaffected.

The SIU mode is able to support architectures in which a single SIU or dual resilient SIU pair are connected into one or more different SS7 networks. The SIU or SIU pair can also independently terminate multiple local point codes within the same network. The following sections describe these different architectures.

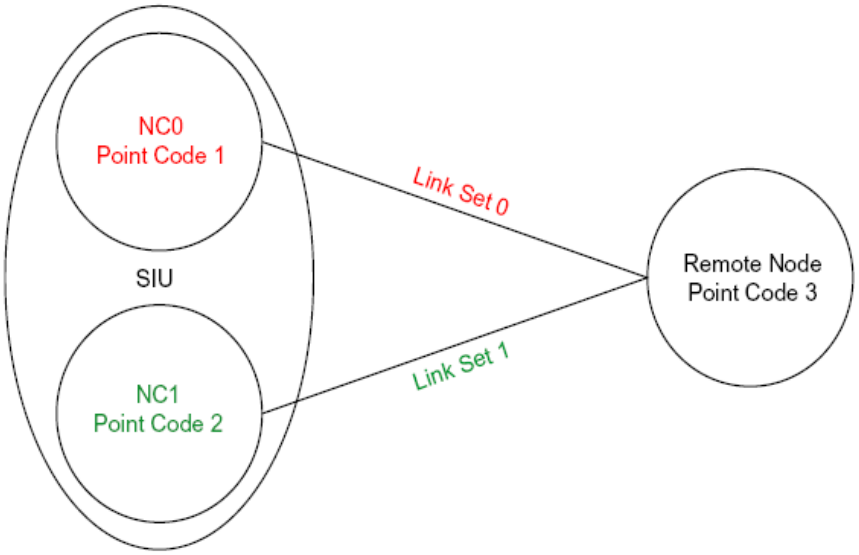
The SIU can support up to four Network Contexts where each Network Context is a different network or different independent local point code within the same network. In the configuration commands or MMI commands, Network Contexts are designated NC0, NC1, NC2 or NC3. Network Context NC0 is also referred to as the default Network Context since this is the Network Context that is assumed if no other explicit value is specified within the command.

7.4.2 Support for Multiple Local Point Codes

In some situations, it is desirable to have an SIU terminate more than one local point code within the same SS7 network. Each local point code can have separate routes and associated pairs of link sets to a destination point code. This means that adding additional local point codes allows additional link sets to be used to send traffic to a destination point code. As link sets are limited to 16 links adding more link sets using multiple local point codes effectively allows a larger total number of links to carry traffic to any single destination point code.

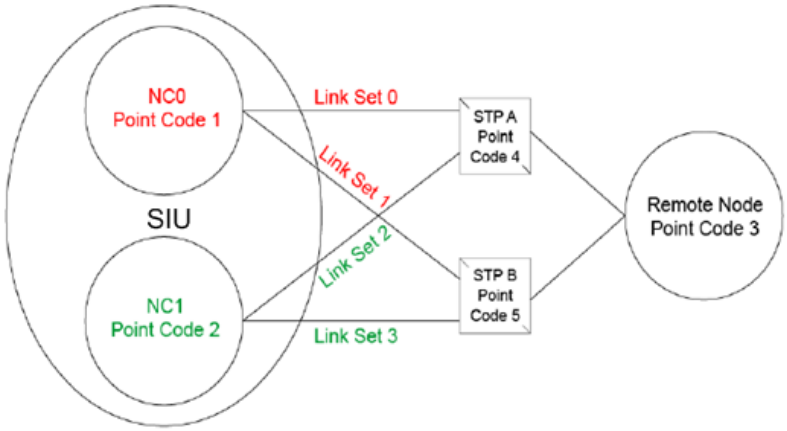
The figure below shows a simple configuration that uses two Network Contexts to allow a single SIU to connect to the remote node using two link sets from two independent local point codes. Link set 0 and 1 are configured in Network Contexts NC0 and NC1 respectively.

Figure 1. Multiple Network Context to Support Multiple Local Point Codes



The figure below extends the previous example to show a configuration with an STP pair. This configuration uses two Network Contexts to allow a single Signaling Server to connect to the Remote Node using four link sets from two independent local point codes. An equivalent configuration using a dual resilient pair is also possible.

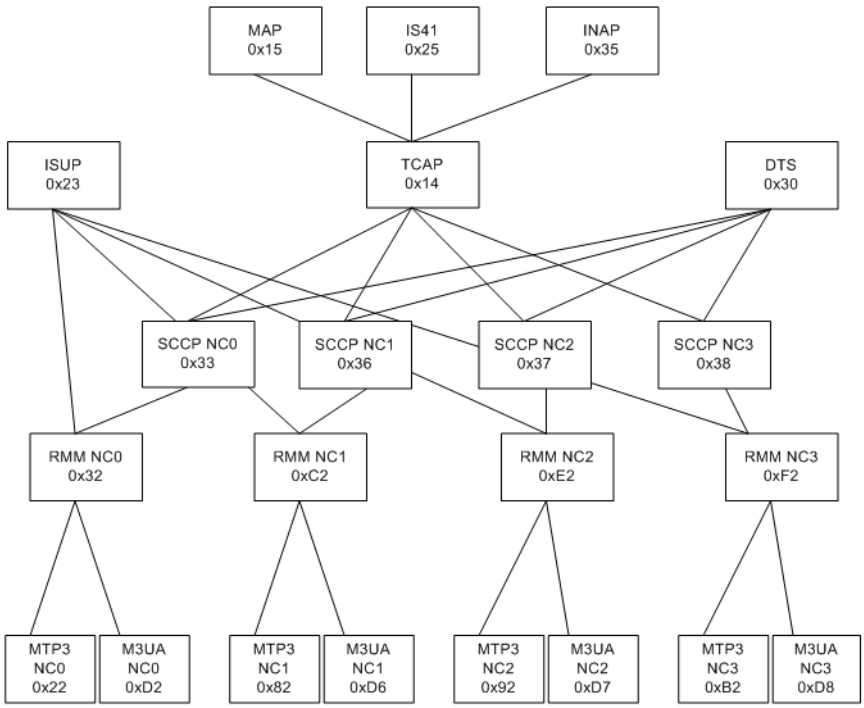
Figure 2. Multiple Network Contexts with an STP Pair



7.4.3 Protocol Handling for Multiple Network Contexts

The figure below shows the use of multiple Network Contexts from an application perspective and provides examples of the module IDs for the various application layers.

Figure 3. Module IDs for Use with Multiple Network Contexts



7.4.4 RMM

MTP3 and M3UA can be active in the same Network Context at the same time. A Destination Point Code must however be unique across all MTP Routes, SIGTRAN Routes and SIGTRAN Remote Application Servers.

On the Signaling Server ISUP and SCCP do not communicate directly with MTP3 and M3UA. Instead they route through a Resilient Management Module (RMM). As well as selecting the correct protocol (MTP3 or M3UA based on DPC) RMM will attempt to route traffic over the inter unit RSI link to the partner Signaling Server if the Destination Point Code cannot be reach via local MTP3/M3UA.

Since there is one instance of RMM for each Network Context, messages that are destined for a specific network must be sent to the correct RMM module ID as shown in the figure above.

In most SIU configurations, RMM is not the highest protocol layer and the sending of messages to the correct module is handled by the higher layer modules without further user interaction.

7.4.5 MTP

7.4.5.1 Applications

Since there is one instance of MTP3 for each Network Context, messages that are destined for a specific network must be sent to the correct MTP module ID as shown in the figure above.

In most Signaling Server configurations, MTP is not the highest protocol layer and the sending of messages to the correct module is handled by the higher layer modules without further user interaction. If an application requires routing at MTP level it is recommended that the application route via the RMM module rather than directly to MTP3.

7.4.5.2 Configuration

The MTP_CONFIG config.txt command, described in “MTP_CONFIG - Global MTP Configuration” on page 71, can be used to configure each Network Context and local point code within the system. NC0 must be configured before NC1, NC2 and NC3 can be configured.

The MTP_ROUTE, MTP_LINKSET and MTP_USER_PART commands support the Network Context-specific NC parameter. This parameter must be specified for all MTP_ROUTE, MTP_LINKSET and MTP_USER_PART commands that are not in the default Network Context (NC0).

7.4.6 M3UA

7.4.6.1 Applications

Since there is one instance of M3UA for each Network Context, messages that are destined for a specific network must be sent to the correct M3UA module ID as shown in the figure above.

In most SIU configurations, M3UA is not the highest protocol layer and the sending of messages to the correct module is handled by the higher layer modules without further user interaction. If an application requires routing at MTP level it is recommended that the application route via the RMM module rather than directly to M3UA.

7.4.6.2 Configuration

The STN_CONFIG config.txt command, described in can be used to configure M3UA in each applicable Network Context. The STN_CONFIG command is required for M3UA in all Network Contexts. NC0 must be configured before NC1, NC2 and NC3 can be configured.

The STN_LINK, STN_LAS, STN_RAS, STN_ROUTE and MTP_USER_PART commands support the Network Context Specific NC parameter. This parameter must be specified for all _LINK, STN_LAS, STN_RAS, STN_ROUTE and MTP_USER_PART commands that are not in the default Network Context (NC0).

7.4.7 ISUP

7.4.7.1 Applications

ISUP applications do not need modification, the config.txt parameters are sufficient to identify the Network Context.

7.4.7.2 Configuration

The ISUP Circuit Group Configuration command, ISUP_CFG_CCTGRP, supports a Network Context-specific NC parameter. This parameter must be used for circuit groups logically assigned to all Network Contexts with the exception of the default Network Context (NC0).

There is no other ISUP-specific Network Context configuration command.

7.4.8 SCCP

7.4.8.1 Applications

In the same manner as MTP3, there is one instance of SCCP for each Network Context; therefore, messages that are destined for a specific network must be sent to the correct SCCP module ID

When TCAP or DTS is used above SCCP, those modules handle the sending of messages to the correct module without further user interaction.

7.4.8.2 Configuration

The SCCP_CONFIG config.txt command, described in Section 5.10.1, “SCCP_CONFIG - SCCP Configuration” on page 116, can be used to configure each Network Context and local point code within the system. NC0 must be configured before NC1, NC2 and NC3 can be configured.

The existing commands SCCP_LSS, SCCP_RSP, SCCP_RSS and SCCP_CONC_SSR include the NC parameter. This parameter must be used for sub-system resources logically assigned to all Network Contexts with the exception of the default Network Context (NC0). For the default Network Context, the value NC0 is optional.

7.4.9 DTS

7.4.9.1 Applications

DTS users should follow the instructions above, which also apply when using DTS. The DTS_ROUTING_REQ message includes a **DTSPN_network_context** parameter that should be used to indicate the network and hence the local point code that a specified sub-system is part of. If this parameter is not specified, the default Network Context, NC0 is assumed.

To route messages to the correct SCCP instance, you must specify the DTC option, DTC_ROUTE_MSG_VIA_DTS. This option is set via bit 0 in the **options** field of the DTC_MSG_CONFIG (0x776c) configuration message.

7.4.9.2 Configuration

There are no DTS-specific Network Context configuration commands.

7.4.10 TCAP

7.4.10.1 Applications

Where a dialog is initiated remotely, no change is required since TCAP automatically determines which Network Context is appropriate. Where the dialog is initiated locally, the application must specify the Network Context to which the message is destined. This effectively indicates the point code to be used as the originating point code.

The Network Context should be indicated in the first message for the dialog being used. In the case of TCAP, this is in the first TCAP service request, typically an Invoke Req, using the TCPPN_NC parameter.

If a Network Context is not specified, the default Network Context, NC0 is assumed.

7.4.10.2 Configuration

The TCAP_CONFIG config.txt command, described in Section 5.13.1, “TCAP_CONFIG - TCAP Configuration” on page 133, can be used to configure the default Network Context for the first network. The TCAP_CONFIG command is only required to alter the TCAP-specific options of the signaling server from the default values, which are determined from the SCCP configuration, and therefore is often not required. Similarly, for each subsequent Network Context, the TCAP_NC_CONFIG command is only required if the TCAP options within that Network Context differ from those determined from the SCCP options within that same Network Context. The TCAP_NC_CONFIG command contains parameters to define address format and TCAP specific options.

The OPTIONS field in the TCAP_NC_CONFIG command takes the same values as that used in the TCAP_CONFIG command. When used to support multiple local point codes within the same network, the OPTIONS settings should typically be the same in both commands. A TCAP_NC_CONFIG command is not required for NC0 since the TCAP_CONFIG command configures the necessary options for the default Network Context.

7.4.11 MAP

7.4.11.1 Applications

Where a dialog is initiated remotely, no change is required since MAP automatically determines which Network Context is appropriate. Where the dialog is initiated locally, the application must specify the Network Context to which the message is destined. This effectively indicates the point code to be used as the originating point code.

The Network Context should be indicated in the first message for the dialog being used. For IS41 the Network Context should be indicated in the Open Request message, instead of using the MAPPN_NC parameter.

If a Network Context is not specified, the default Network Context, NC0 is assumed.

7.4.11.2 Configuration

The MAP_CONFIG config.txt command, described in Section 5.14.1, “MAP_CONFIG - MAP Configuration” on page 137 may be used to configure the default Network Context for the first network. The MAP_CONFIG command is only required to alter the MAP-specific options of the signaling server from the default values and therefore is often not required. Similarly, for each subsequent Network Context the MAP_NC_CONFIG command is only required if the MAP options within that Network Context differ from default values.

The OPTIONS field in the MAP_NC_CONFIG command takes the same values as that used in the MAP_CONFIG command. When used to support multiple local point codes within the same network, the OPTIONS settings should typically be the same in both commands. An MAP_NC_CONFIG command is not required for NC0, since the MAP_CONFIG command configures the necessary options for the default Network Context.

7.4.12 IS41

7.4.12.1 Applications

Where a dialog is initiated remotely, no change is required since IS41 automatically determines which Network Context is appropriate. Where the dialog is initiated locally, the application must specify the Network Context to which the message is destined. This effectively indicates the point code to be used as the originating point code.

The Network Context should be indicated in the first message for the dialog being used. For IS41 the Network Context should be indicated in the Open Request message, instead of using the IS41PN_NC parameter.

If a Network Context is not specified, the default Network Context, NC0 is assumed.

7.4.12.2 Configuration

There are no IS41-specific options, therefore there is no need for an IS41-specific Network Context configuration command.

7.4.13 INAP

7.4.13.1 Applications

Where a dialog is initiated remotely, no change is required since INAP automatically determines which Network Context is appropriate. Where the dialog is initiated locally, the application must specify the Network Context to which the message is destined. This effectively indicates the point code to be used as the originating point code.

The Network Context should be indicated in the first message for the dialog being used. For IS41 the Network Context should be indicated in the Open Request message, instead of using the INAPPN_NC parameter.

If a Network Context is not specified, the default Network Context, NC0 is assumed.

7.4.13.2 Configuration

The existing INAP_CONFIG config.txt command, described in Section 5.16.1, “INAP_CONFIG - INAP Configuration” on page 139 may be used to configure the default Network Context for the first network. The INAP_CONFIG command is only required to alter the INAP specific options of the signaling server from the default values and therefore is often not required. Similarly, for each subsequent Network Context the INAP_NC_CONFIG command is only required if the INAP options within that Network Context differ from default values.

The OPTIONS field in the INAP_NC_CONFIG command takes the same values as that used in the INAP_CONFIG command. When used to support multiple local point codes within the same network, the OPTIONS settings should typically be the same in both commands. An INAP_NC_CONFIG command is not required for NC0 since the INAP_CONFIG command configures the necessary options for the default Network Context.

7.5 Dual Resilient Signaling Server Operation

In order to achieve high availability and a high degree of fault tolerance in an SS7 environment using Dialogic® DSI Signaling Gateways signaling servers, when operating in signaling server mode, an SS7 end point spread over two signaling servers and multiple application servers can be configured and deployed.

Distributing application processing of a signaling point on multiple application servers not only increases the total capacity of a system, but also offers a higher level of fault tolerance in the user application space.

Dialogic® DSI Signaling Servers are designed to support dual-chassis architectures for splitting a point code over two active SS7 nodes. Using this technique, the links in an SS7 link set can be spread between two separate chassis.

This chapter describes the features of the signaling server that are available to build SS7 solutions and reach the five-nines requirements of telco-grade service platforms. It describes the architecture of the Signaling server, reviews potential points of failure of an SS7 system based on the Signaling server, and explains methods to mitigate each of them. This chapter explains the configuration and run-time operation considerations of a dual resilient Signaling server-based system.

There are several well-known methods of achieving this type of reaction to partial failure in the signaling component of communications networks, including:

- Multiple signaling paths (SS7 links and link sets) to each end point
- Distribution of these paths through independent interfaces and cabling
- Distribution of the processing of SS7 terminations at a single signaling point between multiple signaling boards in a single Signaling server
- Physical isolation and duplication of the SS7 interface for a single signaling point on independent protocol engines sharing a single point code
- Splitting the functionality of the application layer between multiple application servers

The first method can be achieved by implementing multiple links (64 Kbps or 56 Kbps channels) between two adjacent inter-communicating points. By definition, these links will be in the same link set. The last two can be accomplished by using two independent, but co-operating signaling servers relaying the SS7 signaling to a distributed application layer split over multiple application hosts.

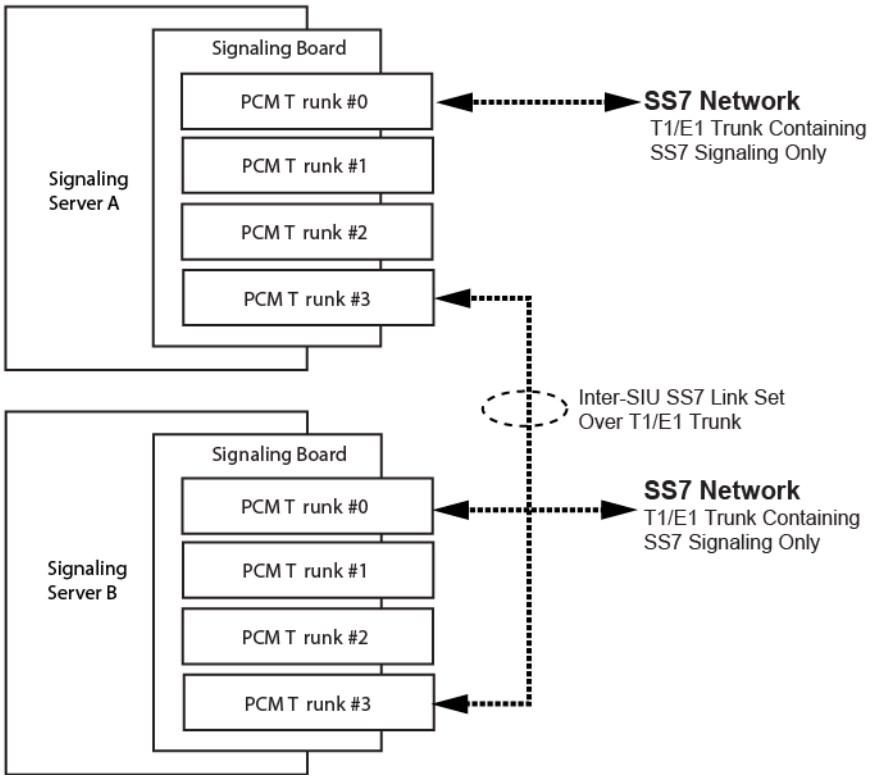
7.5.1 Configuring a Dual Signaling Server Pair

To create a dual resilient configuration for the signaling server, modifications are required to both the system configuration (done using the Man Machine Language [MML] interface) and the protocol configuration (in the config.txt parameter file). This may be done remotely and transferred to the signaling server using FTP.

7.5.2 Hardware Requirements

Configuring a signaling server as one-half of a dual resilient system requires additional hardware ports to carry the inter-signaling server link set between Signaling Server A and Signaling Server B. This may be achieved using T1/E1 interfaces, as shown in Figure 4, or over M2PA between the two units.

Figure 4. Inter-Signaling-Server Link over Crossed T1/E1 Cable



When carried over is carried over a T1/E1 interface, the inter-signaling server signaling link set can be configured to use any signaling processor on any signaling board and may be carried on any of the available interfaces on the signaling board.

7.5.3 System Configuration

The system assignment of Signaling server A or Signaling Server B is made by specifying the MODE parameter in the SIU_DUAL configuration command.

7.5.4 Changes to the config.txt Parameter File

Each signaling server is configured individually. The config.txt parameter file held on each unit reflects the configuration view of the local unit only; hence, assignments of link set and link identities are only unique within a single unit. For the dual resilient configuration the operating mode of the server and the IP address of the other signaling server must be declared using the SIU_DUAL command.

7.5.4.1 Configuring the Inter-Signaling Server Link

The inter-signaling server link set should be defined on both units using the MTP_LINKSET command with bit 15 of the OPTIONS parameter set to 1. This link set must have the same value defined for the OPC and APC values; this will be the local point code of the signaling server pair. Links are added to the inter-signaling server link set using the MTP_LINK command, assigning incrementing REF and SLC values as normal. The BPOS and BLINK parameters define which SS7 processor or signaling processor (SP) channel manages each link.

For a link using a PCM port, the physical location of the link is specified by setting the stream STREAM and timeslot TS.

7.5.4.2 Routing Configuration

A route should be defined on both Signaling Server A and Signaling Server B for the inter-signaling server link set using the MTP_ROUTE command referencing the appropriate linkset LS1 with a DPC value set to the point code of the signaling server pair. This route may only be specified to operate over a single link set.

Each DPC that may be accessed from the application must have an accompanying MTP_ROUTE declaration. For dual resilient operation, each route includes a preferred link set, the LS1 parameter, and a secondary link set specified by LS2. LS1 should reference the link set connecting the signaling server to the appropriate adjacent signaling point, LS2 must be set to the linkset id assigned to the inter-signaling server link set.

7.5.4.3 Circuit Group Configuration

For dual resilient operation, each signaling server should contain identical circuit group declarations using the appropriate ISUP_CFG_CCTGRP command. These circuit group configurations do not become active on either unit until an Activate Circuit Group API command (API_MSG_COMMAND with **cmd_type** = 8) has been issued to a particular signaling server.

7.5.4.4 Example Configuration

To define routing to the DPC 200 in the example following (which is also the adjacent point code), using the first E1 port on the first signaling board in a signaling server, the configuration (Figure 5) would be as follows:

For Signaling Server A:

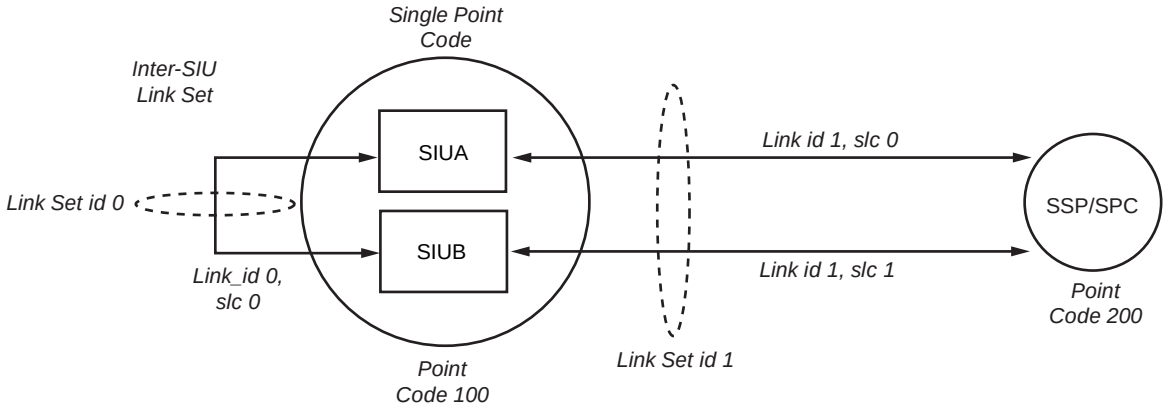
```
*
*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2],[,SSF=0x8],OPTIONS=0][,LABEL=];
MTP_LINKSET:LINKSET=0,OPC=100,APC=100,NLINKS=1,OPTIONS=0x8000,LABEL=To_Partner;
MTP_LINKSET:LINKSET=1,OPC=100,APC=200,NLINKS=1,OPTIONS=0x0000,LABEL=To_Network;
*
*   SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x00000006][,LABEL=];
MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=3,TS=1,OPTIONS=0x00000006;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=2,STREAM=0,TS=16,OPTIONS=0x00000006;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:C7RT=0,DPC=100,LS1=0,UPMASK=0x0020,OPTIONS=0x0000,LABEL=To_Partner;
MTP_ROUTE:C7RT=1,DPC=200,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_Network;
```

For Signaling Server B:

```
*
*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:LINKSET=0,OPC=100,APC=100,NLINKS=1,OPTIONS=0x8000,LABEL=To_Partner;
MTP_LINKSET:LINKSET=1,OPC=100,APC=200,NLINKS=1,OPTIONS=0x0000,LABEL=To_Network;
*
*   SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x00000006][,LABEL=];
MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=3,TS=1,OPTIONS=0x00000006;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=1,SLC=1,BPOS=0,BLINK=2,STREAM=0,TS=16,OPTIONS=0x00000006;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:C7RT=0,DPC=100,LS1=0,UPMASK=0x0020,OPTIONS=0x0000,LABEL=To_Partner;
MTP_ROUTE:C7RT=1,DPC=200,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_Network;
```

Note: The **up_enable** parameter was set for ISUP, user part SI = 5 for the example above.

Figure 5. Example Configuration to an Adjacent SSP / SCP



For a signaling server pair connected to a mated STP pair, carrying the inter-signaling server link over the second E1 port of the first signaling board the configuration (Figure 6) would be:

For Signaling Server A:

```
*
* MTP3 Options Configuration :
* MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG;
*
* SS7 Link Set Configuration :
* MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:LINKSET=0,OPC=300,APC=300,NLINKS=1,OPTIONS=0x8000,LABEL=To_Partner;
MTP_LINKSET:LINKSET=1,OPC=300,APC=400,NLINKS=1,OPTIONS=0x0000,LABEL=To_Network;
*
* SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x00000006][,LABEL=];

MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=3,TS=1,OPTIONS=0x00000006;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=2,STREAM=0,TS=16,OPTIONS=0x00000006;
*
* MTP route Configuration :
* MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:C7RT=0,DPC=300,LS1=0,UPMASK=0x0020,OPTIONS=0x0000,LABEL=To_Partner;
MTP_ROUTE:C7RT=1,DPC=400,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_DPC400;
MTP_ROUTE:C7RT=2,DPC=600,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_DPC600;
```

For Signaling Server B:

```
*
* MTP3 Options Configuration :
* MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG;
*
* SS7 Link Set Configuration :
* MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:LINKSET=0,OPC=300,APC=300,NLINKS=1,OPTIONS=0x8000,LABEL=To_Partner;
MTP_LINKSET:LINKSET=1,OPC=300,APC=500,NLINKS=1,OPTIONS=0x0000,LABEL=To_Network;
*
* SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x00000006][,LABEL=];

MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=3,TS=1,OPTIONS=0x00000006;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=2,STREAM=0,TS=16,OPTIONS=0x00000006;
*
* MTP route Configuration :
* MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:C7RT=0,DPC=300,LS1=0,UPMASK=0x0020,OPTIONS=0x0000,LABEL=To_Partner;
MTP_ROUTE:C7RT=1,DPC=500,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_DPC500;
MTP_ROUTE:C7RT=2,DPC=600,LS1=1,UPMASK=0x0020,OPTIONS=0x0001,LS2=0,LABEL=To_DPC600;
```

Figure 6. Example Configuration to an Adjacent STP Pair

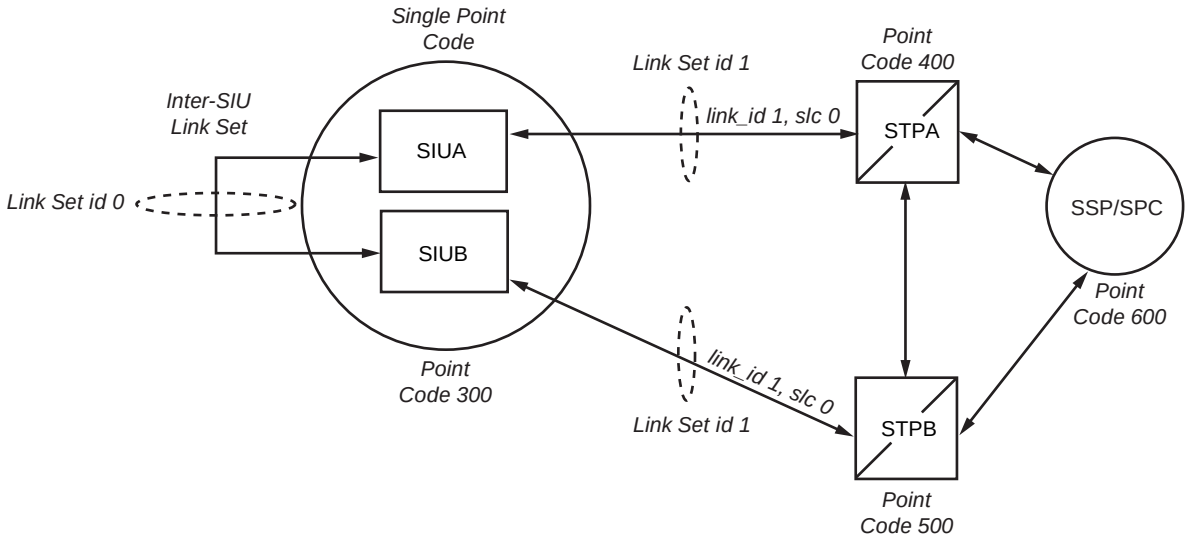
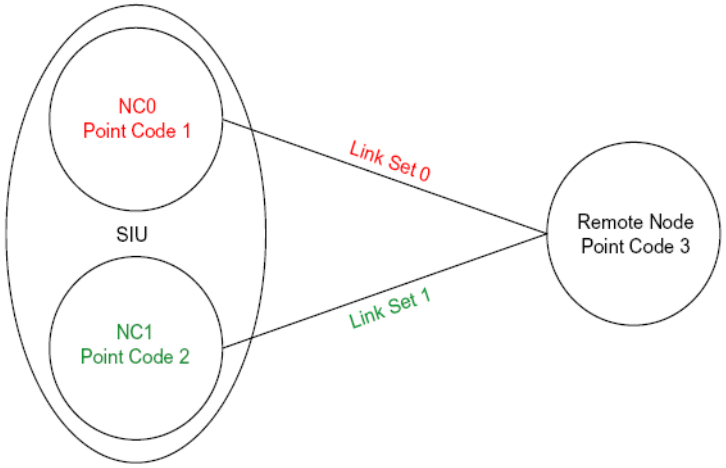


Figure 7. Multiple Local Point Code Configuration Example



The example config.txt file below shows the configuration of a system based on the figure above.

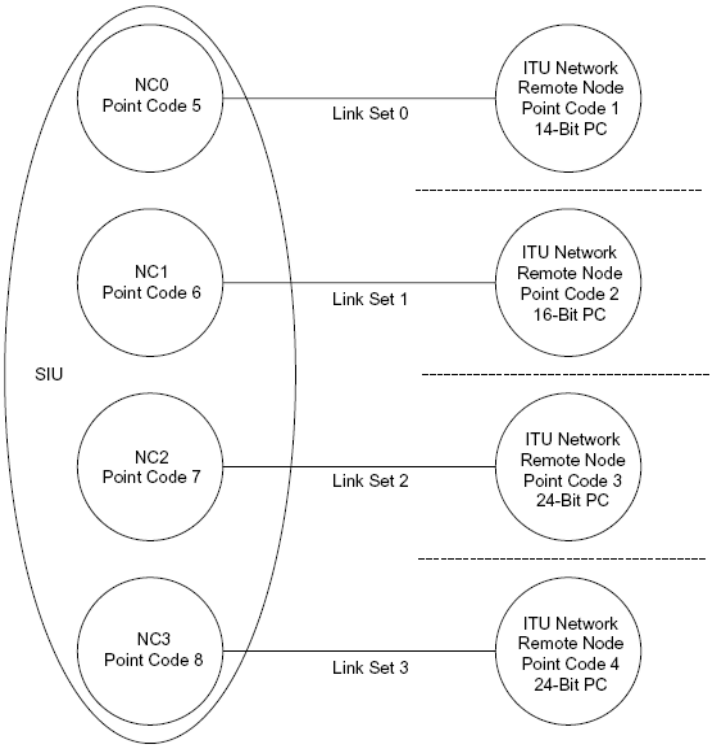
```
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   Signaling Board Configuration :
*   SS7_BOARD:BPOS=,BRDTYPE=,OPTIONS=;
SS7_BOARD:BPOS=0,BRDTYPE=SS7MD,OPTIONS=0x00000001;
SS7_BOARD:BPOS=1,BRDTYPE=SS7MD,OPTIONS=0x00000001;
*
*   T1/E1 PCM network interface trunk Configuration :
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=E1[,LC=HDB3][,FF=G704][,CRC_MODE=NONE][,BUILDOUT=0][,OPTIONS=0][,LABEL
=];
*     or
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=T1[,LC=B8ZS][,FF=ESF][,CRC_MODE=NONE][,BUILDOUT=1][,OPTIONS=0][,LABEL=
];
```

```
LIU_CONFIG:PORTID=0,PCM=0-1,LIUTYPE=E1;
LIU_CONFIG:PORTID=4,PCM=1-1,LIUTYPE=E1;
*
*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG:NC=NC0,OPTIONS=0x0002;
MTP_CONFIG:NC=NC1,OPTIONS=0x0002;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:NC=NC0,LINKSET=0,OPC=1,APC=3;
MTP_LINKSET:NC=NC1,LINKSET=1,OPC=2,APC=3;
*
*   SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=],STREAM=,TS=[,OPTIONS=0x00000006][,LABEL=];
MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=0,STREAM=0,TS=16;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=0,REF=1,SLC=1,BPOS=1,BLINK=0,STREAM=0,TS=16;

MTP_LINK:LINK=2,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=0,TS=17;
MTP_LINK:LINK=3,IFTYPE=TDM,LINKSET=1,REF=1,SLC=1,BPOS=1,BLINK=1,STREAM=0,TS=17;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:NC=NC0,C7RT=0,DPC=3,LS1=0,UPMASK=0x0008;
MTP_ROUTE:NC=NC1,C7RT=1,DPC=3,LS1=1,UPMASK=0x0008;
*
*
*   SCCP Options Configuration :
*   SCCP_CONFIG:[NC=NC0],OPC=[,SSF=0x8][,OPTIONS=0][,OPTIONS2=0x00000001];
SCCP_CONFIG:NC=NC0,OPC=1,OPTIONS=0x0126;
SCCP_CONFIG:NC=NC1,OPC=2,OPTIONS=0x0126;
*
*   Sub-System Resource Configuration :
*   SCCP_LSS:[NC=NC0],SSRID=, SSN=,LSSPROT=[,USER_ID=0x1d][,OPTIONS=0][,LABEL=];
*     or
*   SCCP_RSP:[NC=NC0],SSRID=,SPC=[,OPTIONS=0][,PCMASK=0][,LABEL=];
*     or
*   SCCP_RSS:[NC=NC0],SSRID=,SPC=,SSN=[,OPTIONS=0][,LABEL=];
SCCP_LSS:NC=NC0,SSRID=0,SSN=8,USER_ID=0x1d,LSSPROT=INAP;
SCCP_RSP:NC=NC0,SSRID=1,SPC=3;
SCCP_RSS:NC=NC0,SSRID=2,SPC=3,SSN=8;

SCCP_LSS:NC=NC1,SSRID=3,SSN=8,USER_ID=0x1d,LSSPROT=INAP;
SCCP_RSP:NC=NC1,SSRID=4,SPC=3;
SCCP_RSS:NC=NC1,SSRID=5,SPC=3,SSN=8;
*
*   INAP Options Configuration :
*   INAP_CONFIG:[NC=NC0][,OPTIONS=0];
INAP_CONFIG:NC=NC0;
INAP_CONFIG:NC=NC1;
*
*
*
*   End of file
*
```

Multiple Network Configuration Example

The Network Context-based configuration of the SIU mode allows the settings and behavior to be configured independently for each Network Context. This allows a system to be configured with mixed ITU and ANSI network types or allows multiple networks of the same type to configured with different settings.

Figure 8. Multiple Network Configuration Example



The example config.txt file below shows the configuration of a system based on the figure above.

```
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   Signaling Board Configuration :
*   SS7_BOARD:BPOS=,BRDTYPE=,OPTIONS=;
SS7_BOARD:BPOS=0,BRDTYPE=SS7MD,OPTIONS=0x00000001;
SS7_BOARD:BPOS=1,BRDTYPE=SS7MD,OPTIONS=0x00000001;
*
*   T1/E1 PCM network interface trunk Configuration :
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=E1[,LC=HDB3][,FF=G704][,CRC_MODE=NONE][,BUILDOUT=0][,OPTIONS=0][,LABEL
=];
*     or
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=T1[,LC=B8ZS][,FF=ESF][,CRC_MODE=NONE][,BUILDOUT=1][,OPTIONS=0][,LABEL=
];
LIU_CONFIG:PORTID=0,PCM=0-3,LIUTYPE=E1;
LIU_CONFIG:PORTID=1,PCM=0-4,LIUTYPE=E1;
LIU_CONFIG:PORTID=2,PCM=1-3,LIUTYPE=T1;
LIU_CONFIG:PORTID=3,PCM=1-4,LIUTYPE=T1;

LIU_CONFIG:PORTID=4,PCM=0-1,LIUTYPE=T1;
```

```
LIU_CONFIG:PORTID=5,PCM=1-1,LIUTYPE=T1;

*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
*   options bits 8,10 and 11 set to 1 it is ANSI operation
*   options bit 9 if set to 1 pc is 24 bit else it is 14/16 bit
*   options bit 20 if set to 1 pc is 16 bit if bit 9 not set
MTP_CONFIG:NC=NC0,OPTIONS=0x00010000;
MTP_CONFIG:NC=NC1,OPTIONS=0x00110C08;
MTP_CONFIG:NC=NC2,OPTIONS=0x00010F08;
MTP_CONFIG:NC=NC3,OPTIONS=0x00010200;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:NC=NC0,LINKSET=0,OPC=5,APC=1,OPTIONS=0;
MTP_LINKSET:NC=NC1,LINKSET=1,OPC=6,APC=2,OPTIONS=0;
MTP_LINKSET:NC=NC2,LINKSET=2,OPC=7,APC=3,OPTIONS=0,SSF=0xB;
MTP_LINKSET:NC=NC3,LINKSET=3,OPC=8,APC=4,OPTIONS=0;

MTP_LINKSET:NC=NC0,LINKSET=4,OPC=5,APC=5,OPTIONS=0x8000;
MTP_LINKSET:NC=NC1,LINKSET=5,OPC=6,APC=6,OPTIONS=0x8000;
MTP_LINKSET:NC=NC2,LINKSET=6,OPC=7,APC=7,OPTIONS=0x8000,SSF=0xB;
MTP_LINKSET:NC=NC3,LINKSET=7,OPC=8,APC=8,OPTIONS=0x8000;
*
*   SS7 Link Configuration :
*
*MTP_LINK:LINK=,IFTYPE=TDM,LINKSET=,REF=,SLC=,BPOS=,BLINK=0,STREAM=[,TS=][,OPTIONS=0x00000006][,LABEL=
];
MTP_LINK:LINK=0,IFTYPE=TDM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=0,STREAM=2,TS=16;
MTP_LINK:LINK=1,IFTYPE=TDM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=1,STREAM=3,TS=16;
MTP_LINK:LINK=2,IFTYPE=TDM,LINKSET=2,REF=0,SLC=0,BPOS=1,BLINK=0,STREAM=2,TS=24;
MTP_LINK:LINK=3,IFTYPE=TDM,LINKSET=3,REF=0,SLC=0,BPOS=1,BLINK=1,STREAM=3,TS=24;

MTP_LINK:LINK=4,IFTYPE=TDM,LINKSET=4,REF=0,SLC=0,BPOS=0,BLINK=2,STREAM=0,TS=1;
MTP_LINK:LINK=5,IFTYPE=TDM,LINKSET=7,REF=0,SLC=0,BPOS=0,BLINK=3,STREAM=0,TS=2;
MTP_LINK:LINK=6,IFTYPE=TDM,LINKSET=5,REF=0,SLC=0,BPOS=1,BLINK=2,STREAM=0,TS=1;
MTP_LINK:LINK=7,IFTYPE=TDM,LINKSET=6,REF=0,SLC=0,BPOS=1,BLINK=3,STREAM=0,TS=2;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:NC=NC0,C7RT=0,DPC=1,LS1=0,UPMASK=0x07f8;
MTP_ROUTE:NC=NC1,C7RT=1,DPC=2,LS1=1,UPMASK=0x07f8;
MTP_ROUTE:NC=NC2,C7RT=2,DPC=3,LS1=2,UPMASK=0x07f8;
MTP_ROUTE:NC=NC3,C7RT=3,DPC=4,LS1=3,UPMASK=0x07f8;

MTP_ROUTE:NC=NC0,C7RT=4,DPC=5,LS1=4,UPMASK=0x07f8;
MTP_ROUTE:NC=NC1,C7RT=5,DPC=6,LS1=5,UPMASK=0x07f8;
MTP_ROUTE:NC=NC2,C7RT=6,DPC=7,LS1=6,UPMASK=0x07f8;
MTP_ROUTE:NC=NC3,C7RT=7,DPC=8,LS1=7,UPMASK=0x07f8;
*
*   MTP_USER_PART [NC] <SI> <USER_ID>
MTP_USER_PART NC0 8 0x1d
MTP_USER_PART NC1 7 0x2d
MTP_USER_PART NC2 6 0x3d
MTP_USER_PART NC3 5 0x4d
*
*   End of file
```

7.5.5 Configuring a Dual Resilient System

For the dual resilient configuration, it is necessary to modify the configuration to assign one unit as MODEA and the other as MODEB using the SIU_DUAL configuration command. The command should also be used to specify the IP address of the partner system.

The inter-SIU link set should be defined on both units using the MTP_LINKSET command with bit 15 of the OPTIONS parameter set to 1. This link set must have the same value defined for the OPC and APC values; this is the local point code of the SIU pair. Links are added to the Inter-SIU link set using the MTP_LINK command, assigning incrementing REF and SLC values as used normally. The BPOS and BLINK parameters should be set accordingly.

A route should be defined on each unit for the inter-signaling server link set using the MTP_ROUTE command referencing the appropriate LINKSET with a DPC value set to the point code of the SIU pair.

The management entity within each signaling server indicates the availability of the inter-signaling server links to the application running on the first host using the message based Application Programming Interface (API).

Additional information for the protocol configuration commands and parameters may be found in the previous sections.

7.6 Configuring an ANSI System

This section provides additional guidelines for configuring an Signaling Server to operate in accordance with the ANSI T1 specifications.

The default protocol configuration for an Signaling Server specifies ITU-T protocol behavior. To operate in accordance with ANSI it is necessary to modify the options settings for MTP3 and the User Part held in the protocol configuration file on the Signaling Server.

The MTP_CONFIG OPTIONS parameter must have bits 8 to 11 set to 1 (value 0x0f00) to define ANSI operation.

The MTP_LINKSET SSF parameter must have the least two significant bits (B and A) both set to 1 so that all MTP3 originated messages are assigned a message priority of 3. The two most significant bits (D and C) are the network indicator. Hence valid ANSI ssf values are 0x3, 0x7, 0xb and 0xf.

ANSI operation for the protocol layers above MTP3 is specified using the configuration values specified in the Configuration Section of the appropriate programmer's manual.

The CIC_MASK parameter in the example User Part circuit group configuration commands (ISUP_CFG_CCTGRP) define groups containing 30 B-channels with timeslot 16 being unavailable for telephony traffic, corresponding to a 30B+D E1 bearer. This would have a CIC pattern mask of 0x7fff7fff. T1 bearers provide 24 channels, hence for a 23B+D T1 span, with timeslot 24 used for the D channel (SS7) operation, the CIC pattern mask should be modified to 0x7fffff.

The TS parameter in the example cross connect command applies to an E1 (32-timeslot) PCM connection. This should be modified to reference 24 timeslots for a T1 configuration. Hence, to apply a cross connect to timeslots 1 to 23, (leaving timeslot 24 for SS7) the mask should be set to 0x1ffffe.

Additional information for the protocol configuration commands and parameters may be found in the previous sections.

7.7 Specifying Default Routes

For telephony operation, the Signaling Server requires an MTP_ROUTE definition for each signaling point that the local point code(s) communicate with. In addition, transaction-based systems require a declaration of each remote sub-system with an SCCP_RSS command.

It is also possible to configure MTP routes that are designated as “default” routes. Default routes can be used to convey traffic for multiple destinations without the need to configure each Destination Point Code (DPC) as an explicit MTP route. Typically, this is useful when a signaling point connects simply to a single STP or a mated pair of STPs and all traffic can be sent to the STP, irrespective of current network status.

Two types of default route are supported:

- One associated with a “real” DPC. In this case the (default) route is deemed to be accessible whenever the specified DPC is accessible.
- One associated with a “pseudo” DPC, which is a point code that does not exist within the network (for example, zero). In this case the (default) route is deemed to be accessible as soon as the link sets within the route are available.

A maximum of one default route for each supported Service Indicator (or user part) is permitted. Configuration of default routes utilizes bits 2, 3, and 5 in the OPTIONS field of the MTP_ROUTE command.

For transaction based applications, it is also necessary to supply a <pc_mask> value with the definition of each SCCP_RSS. The PCMASK is used to determine which bits of the target point code (the destination point code in the MTP label of the transmit message) should be ignored when selecting the route. The PCMASK makes it possible to configure a route to a specific destination that is also used for other destinations with a similar point code. This allows configuration of default destination sub-systems (for example, to a gateway SCP).

7.8 Dynamic Host Activation

The Signaling Server when acting as an SIU has the ability to activate/deactivate host links using the MNINI/MNINE commands. This functionality supports the preservation of the host status over a restart and no alarms are reported for those hosts that have been deactivated.

If the SIU_HOSTS configuration command is omitted from the configuration file then the number of hosts is determined from what has been configured in MMI.

If the SIU_HOSTS configuration command is present and NUM_HOSTS is set to ALL then all host links are configured, but only one host link is activated (the others remain deactivated initially).

If the SIU_HOSTS configuration command is present and NUM_HOSTS is set to a value other than ALL, then that number of hosts are configured and activated; in this case, no additional hosts can be configured.

This allows the SIU users to escalate their systems by adding or removing host connections at runtime and without the need to apply a system restart to the unit. In the case that a unit restart is required, the configuration adopted can be preserved.

7.9 Dynamic Configuration

Dynamic configuration allows you to add, delete, or modify configuration elements (for example, circuit groups) without affecting the state of any other configuration element in the system. Dynamic configuration does not require a system restart. There are two forms of dynamic configuration:

- Config.txt-based dynamic configuration, where the user transmits an updated config.txt file to the system, then executes an MMI command to load the configuration into system memory for use. Since the new configuration exists within a config.txt file, the updated configuration is preserved over a restart. See below for more information.
- Application-based dynamic configuration, where a user application transmits a configuration message directly to the protocol module. Since the new configuration does not exist in a config.txt file, the updated configuration is not preserved over a restart and it is therefore necessary for the user application to detect any restart of the Signaling Server and reconfigure the unit as needed.

7.9.1 Config.txt-Based Dynamic Configuration

In config.txt-based dynamic configuration, the user transmits an updated config.txt file to the system, then executes an MMI command to load the configuration into system memory for use. Since the new configuration exists within a config.txt file, the updated configuration is preserved over a restart.

The process for config.txt-based dynamic configuration is as follows:

1. Add, delete, or modify the configuration element in the config.txt file.
2. Transfer the config.txt file to the unit via FTP.
3. Invoke the specific MMI command (e.g., MTP link add - CNSLI) to update the unit configuration.

In every case when the Signaling Server is restarted, the configuration file last transferred will be applied to the unit.

The dynamic configuration update commands return the following responses:

- RANGE ERROR - the identifier value is invalid
- UNACCEPTABLE COMMAND - the command does not satisfy all prerequisite conditions
- GENERAL ERROR - the config.txt command line is incorrectly formatted or the operation failed to complete successfully – the configuration of the system is restored to the state prior to command execution.

Note the following:

- When adding configuration elements, the elements may not already be configured within the Signaling Server.
- When changing or deleting configuration elements, the elements must already have been previously configured within the Signaling Server.
- When using dynamic configuration all command line parameters, including the element identifier value, are mandatory. Dynamic configuration may fail if the format of the command line does not include all the parameters identified in this manual.

The majority of config.txt commands support dynamic configuration, see the specific config.txt command to see whether it is supported and what MMI command is required to perform the update.

7.10 SIGTRAN M2PA Signaling

7.10.1 Overview

The Signaling Server supports the SIGTRAN M2PA protocol compatible with IETF RFC 4165. M2PA peer- to-peer operation can be employed as the network transport layer, providing services normally provided by MTP2 for SS7 signaling links.

SS7 signaling traffic can be conveyed over SIGTRAN network-facing links to a signaling gateway or other signaling point employing M2PA. In dual configuration, an M2PA link can be used as the Signaling Server interlink to carry SS7 data between the two units.

Using the STN_LINK command, you can configure up to 256 M2PA links. The STN_LINK command should appear before the MTP_CONFIG command in the config.txt file. Having configured an M2PA link, you can associate this with an SS7 link using the MTP_LINK command.

7.10.2 M2PA License

Before M2PA network facing links can be configured, the unit must be equipped with an M2PA license, as listed in Section 2.1.3, “Temporary Licenses” on page 15.

The M2PA license is not required for configuration of M2PA interlinks employed in Signaling Server dual configuration. With the license installed, the CNSYP command will display the M2PA parameter set to Y. Without a license the CNSYP command will not display the M2PA parameter.

7.10.3 SS7 over M2PA

An SS7 link is associated with the M2PA link using the MTP_LINK command. SS7 MSUs will then be carried over SIGTRAN as opposed to MTP2.

An SS7 link can only be associated with one M2PA link, and two SS7 links cannot be associated with the same M2PA link. The following commands demonstrate M2PA and SS7 link configuration.

```
STN_LINK:SNLINK=1,SNTYPE=M2PA,RIP1=192.168.1.2,LIP1=192.168.1.1,END=C,LPORT=3565,RPORT=3565,M2PAID=1;
MTP_LINK:LINK=1,IFTYPE=M2PA,LINKSET=1,REF=0,SLC=0,BLINK=1,OPTIONS=0x00000006;
```

The SS7 link is associated with an M2PA link IFTYPE is set to M2PA. The BLINK parameter identifies the M2PA link SNLINK.

7.10.4 Configuration Examples

Example configuration of SS7 links conveyed over M2PA.

```
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   SIGTRAN Link Configuration :
*STN_LINK:SNLINK=,SNTYPE=M2PA,RIP1=[,RIP2=],LIP1=[,LIP2=][,END=S][,LPORT=3565][,RPORT=3565][,OPTIONS=0
],M2PAID=[,LABEL=];
STN_LINK:SNLINK=1,SNTYPE=M2PA,RIP1=192.168.1.2,LIP1=192.168.1.1,END=C,LPORT=3565,RPORT=3565,M2PAID=1;
STN_LINK:SNLINK=2,SNTYPE=M2PA,RIP1=192.168.1.2,LIP1=192.168.1.1,END=C,LPORT=3566,RPORT=3566,M2PAID=2;
STN_LINK:SNLINK=99,SNTYPE=M2PA,RIP1=192.168.1.2,LIP1=192.168.1.1,END=C,LPORT=3567,RPORT=3567,M2PAID=99
;
*
*
*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:LINKSET=1,OPC=300,APC=400,NLINKS=1,LABEL=To_Network;
```

```
*
*   SS7 Link Configuration :
*   MTP_LINK:LINK=,IFTYPE=M2PA,LINKSET=,REF=,SLC=[,BLINK=][,OPTIONS=0x00000006][,LABEL=];
MTP_LINK:LINK=1,IFTYPE=M2PA,LINKSET=1,REF=0,SLC=0,BLINK=1,OPTIONS=0x00000006;
MTP_LINK:LINK=2,IFTYPE=M2PA,LINKSET=1,REF=1,SLC=1,BLINK=2,OPTIONS=0x00000006;
MTP_LINK:LINK=99,IFTYPE=M2PA,LINKSET=1,REF=2,SLC=2,BLINK=99,OPTIONS=0x00000006;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:C7RT=0,DPC=400,LS1=1,UPMASK=0x0028;
```

7.11 SIGTRAN M3UA Signaling

7.11.1 Overview

This Signaling Server supports the SIGTRAN M3UA protocol compatible with IETF RFC 4666. M3UA can be deployed as a direct replacement for MTP3 on the Signaling Server with M3UA over SCTP offering a SS7 over IP solution removing the need to deploy TDM SS7 links.

Using M3UA, the Signaling Server can connect either directly to multiple Signaling End Points (SEPs) in a IPSP (peer to peer) configuration, or indirectly via a SIGTRAN Signaling Gateway. M3UA supports load-sharing across a pair of Signaling Server Signaling Servers, configured as a single point code, without the requirement for a TDM Signaling Server interlink between the two units.

M3UA must be configured to operate in a particular network context using the STN_NC command. MTP and M3UA may be configured in the same network context but must be configured to route to different Destination point Codes.

When a Signaling Server is using M3UA, it is considered be acting as one or more Local Application Servers. Using the STN_LINK command, you can configure up to 256 M3UA links. These links may be connected to either a SIGTRAN Signaling Gateway using the STN_LINK command, or up to 256 Remote Application Servers (Signaling End Points) using the STN_RAS and STN_RASLIST commands. When interworking to a SIGTRAN Signaling Gateway, the Signaling Server can be configured to route to up to 256 Remote Point Codes in the network, using the Signaling Gateway with the STN_ROUTE and STN_RSGLIST commands. Finally, the Local Application Server can be associated with either a Remote Application Server or Signaling Gateway, using the STN_LBIND command.

7.11.2 Configuration Examples

SIU to Signaling Gateway

Example configuration of an SIU acting as Point Code 3 communicating to point code 2 via a Signaling Gateway.

```
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   M3UA Options Configuration :
*   STN_CONFIG:[NC=NC0],SS7MODE=[,OPTIONS=0][,SHARE=100];
STN_CONFIG:SS7MODE=ITU14;
*
*   SIGTRAN Local Application Server Configuration :
*   STN_LAS:[NC=NC0],LAS=,OPC=,RC=[,TRMD=LS][,OPTIONS=0][,LABEL=];
STN_LAS:LAS=1,OPC=3,RC=1;
*
*   SIGTRAN Link Configuration :
*
*STN_LINK:[NC=NC0],SNLINK=,SNTYPE=M3UA,RIP1=[,RIP2=],LIP1=[,LIP2=][,END=S][,LPORT=2905][,RPORT=2905][,
OPTIONS=0][,RSG=][,NA=][,LABEL=];
```

```
STN_LINK:SNLINK=1,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=S,LPORT=2905,RPORT=2905,OPTI
ONS=0x0006,RSG=1;
STN_LINK:SNLINK=2,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=S,LPORT=2906,RPORT=2906,OPTI
ONS=0x0006,RSG=1;
*
*   SIGTRAN Route Configuration :
*   STN_ROUTE:[NC=NC0],SNRT=,DPC=[,OPTIONS=0][,LABEL=];
STN_ROUTE:SNRT=1,DPC=2;
*
*   SIGTRAN Gateway List Configuration :
*   STN_RSGLIST:GLID=,SNRT=,RSG=[,OPTIONS=0];
STN_RSGLIST:GLID=1,SNRT=1,RSG=1;
*
*   SIGTRAN Bind Configuration :
*   STN_LBIND:BIND=,LAS=[,RAS=][,RSG=][,OPTIONS=0];
STN_LBIND:BIND=1,LAS=1,RSG=1;
*
```

SIU to Remote Application Server (IPSP Operation)
Example configuration of an SIU in IPSP operation using 4 links to connect with 2 Remote Application Servers.

```
*   M3UA config to connect SIU to 2 RAS (IPSP)using 4 LINKS
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   M3UA Options Configuration :
*   STN_CONFIG:[NC=NC0],SS7MODE=[,OPTIONS=0][,SHARE=100];
STN_CONFIG:SS7MODE=ITU14;
*
*   SIGTRAN Local Application Server Configuration :
*   STN_LAS:[NC=NC0],LAS=,OPC=,RC=[,TRMD=LS][,OPTIONS=0][,LABEL=];
STN_LAS:LAS=0,OPC=100,RC=1;
STN_LAS:LAS=1,OPC=100,RC=2;

*
*   SIGTRAN Link Configuration :
*
*STN_LINK:[NC=NC0],SNLINK=,SNTYPE=M3UA,RIP1=[,RIP2=],LIP1=[,LIP2=][,END=S][,LPORT=2905][,RPORT=2905][,
OPTIONS=0][,RSG=][,NA=][,LABEL=];
STN_LINK:SNLINK=0,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=C,LPORT=2905,RPORT=2905;
STN_LINK:SNLINK=1,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=C,LPORT=2906,RPORT=2906;
STN_LINK:SNLINK=2,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=C,LPORT=2907,RPORT=2907;
STN_LINK:SNLINK=3,SNTYPE=M3UA,RIP1=192.168.17.200,LIP1=192.168.17.201,END=C,LPORT=2908,RPORT=2908;
*   SIGTRAN Remote Application Server Configuration :
*   STN_RAS:[NC=NC0],RAS=,DPC=,RC=[,NASP=1][,OPTIONS=0][,LABEL=];
STN_RAS:RAS=0,DPC=10,RC=1;
STN_RAS:RAS=1,DPC=11,RC=1;

*
*   SIGTRAN Remote Application Server List Configuration :
*   STN_RASLIST:RLID=,RAS=,SNLINK=;
STN_RASLIST:RLID=0,RAS=0,SNLINK=0;
STN_RASLIST:RLID=1,RAS=0,SNLINK=1;
STN_RASLIST:RLID=2,RAS=1,SNLINK=2;
STN_RASLIST:RLID=3,RAS=1,SNLINK=3;
*
*   SIGTRAN Bind Configuration :
*   STN_LBIND:BIND=,LAS=[,RAS=][,RSG=][,OPTIONS=0];
STN_LBIND:BIND=0,LAS=0,RAS=0;
STN_LBIND:BIND=1,LAS=1,RAS=1;
*
* User part configuration e.g. ISUP or SCCP.
```

7.12 SIGTRAN M3UA - Dual Operation

M3UA on a pair of Signaling Server s can offer a level of resilience similar to that supported by a pair of Signaling Server s operating MTP3. When configured, the Signaling Servers will each behave as an Application Server Process operating within an Application Server; thus presenting a single point code to the network.

In the same manner as MTP3 resilient operation, one Signaling Server should be configured as MODEA and the other as MODEB using the SIU_DUAL configuration command. The command should also be used to be configure the IP address of the partner Signaling Server.

Unlike MTP3 there is no need to specify any further configuration for inter Signaling Server communication (i.e., inter unit links or linksets), M3UA within the Signaling Server pair will use the inter Signaling Server Ethernet link to maintain communication with the network even when a single Signaling Server loses direct communication to an adjacent server (Signaling Gateway or IPSP).

Dual resilient operation using M3UA does require load-sharing which is based on SLS value. Load-sharing should be configured using the STN_LAS command on both units.

7.13 ATM Configuration

7.13.1 Overview

The use of an SS7MDL4 board in the Signaling Server means that, in addition to supporting traditional Low Speed Links at 64, 56 or 48kbps and High Speed Links in accordance with Q.703 Annex A, the Signaling Server can also connect over E1 or T1 to ATM networks.

The Signaling Server supports termination of ATM (Q.SAAL) links. It also supports the ability to monitor ATM links at the AAL5 layer and allows the resulting monitored traffic to be sent to a specific SIU host for each AAL5 link.

The board supports software selectable high impedance or protective monitoring point mode for use in conjunction with monitoring.

ATM link termination is implemented in accordance with Q.SAAL (Q.2140/Q.2110/GR-2878).

7.13.2 Configuration Example

The following example configuration shows two ATM signaling links looped back on the Signaling Server (LIU 1-1 to LIU 1-2 and LIU 1-3 to LIU 1-4), where the SIU acts as point codes 1 and 2. Four cell stream and MTP links are configured showing configuration for either side of the two Signaling Links.

```
*
*   Signaling Server Host Configuration Change :
*   SIU_HOSTS:NUM_HOSTS=,BACKUP_HOST=,OPTIONS=,MIN_HOSTS=,DMHOST=;
SIU_HOSTS:NUM_HOSTS=1,BACKUP_HOST=NONE,OPTIONS=0,MIN_HOSTS=1,DMHOST=0;
*
*   Signaling Board Configuration :
*   SS7_BOARD:BPOS=,BRDTYPE=,OPTIONS=;
SS7_BOARD:BPOS=0,BRDTYPE=SS7MD,OPTIONS=0x00000001;
*
*   T1/E1 PCM network interface trunk Configuration :
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=E1[,LC=HDB3][,FF=G704][,CRC_MODE=NONE][,BUILDOUT=0][,OPTIONS=0][,LABEL
=];
*     or
*
LIU_CONFIG:PORTID=,PCM=,LIUTYPE=T1[,LC=B8ZS][,FF=ESF][,CRC_MODE=NONE][,BUILDOUT=1][,OPTIONS=0][,LABEL=
];
```

```
LIU_CONFIG:PORTID=0,PCM=0-1,LIUTYPE=E1;
LIU_CONFIG:PORTID=1,PCM=0-2,LIUTYPE=E1;
LIU_CONFIG:PORTID=2,PCM=0-3,LIUTYPE=E1;
LIU_CONFIG:PORTID=3,PCM=0-4,LIUTYPE=E1;
*
*   ATM Cell Stream Configuration :
*   ATM_CELL_STREAM:CELLSTR=,BPOS=,L2ID=,PORTID=[,OPTIONS=0x0006],DEFVPI=,DEFVCI=;
ATM_CELL_STREAM:CELLSTR=0,BPOS=0,L2ID=0,PORTID=0,DEFVPI=1,DEFVCI=6;
ATM_CELL_STREAM:CELLSTR=1,BPOS=0,L2ID=1,PORTID=1,DEFVPI=1,DEFVCI=6;
ATM_CELL_STREAM:CELLSTR=2,BPOS=0,L2ID=2,PORTID=2,DEFVPI=1,DEFVCI=6;
ATM_CELL_STREAM:CELLSTR=3,BPOS=0,L2ID=3,PORTID=3,DEFVPI=1,DEFVCI=6;
*
*   MTP3 Options Configuration :
*   MTP_CONFIG:[NC=NC0][,OPTIONS=0];
MTP_CONFIG:NC=NC0,OPTIONS=0x0002;
MTP_CONFIG:NC=NC1,OPTIONS=0x0002;
*
*   SS7 Link Set Configuration :
*   MTP_LINKSET:[NC=NC0],LINKSET=,OPC=,APC=[,NLINKS=2][,SSF=0x8][,OPTIONS=0][,LABEL=];
MTP_LINKSET:NC=NC0,LINKSET=0,OPC=1,APC=3;
MTP_LINKSET:NC=NC1,LINKSET=1,OPC=2,APC=3;
*
*   SS7 Link Configuration :
*
MTP_LINK:LINK=,IFTYPE=ATM,LINKSET=,REF=,SLC=[,BPOS=][,BLINK=][,OPTIONS=0x00000006],CELLSTR=,VPI=,VCI=[
,LABEL=];
MTP_LINK:LINK=0,IFTYPE=ATM,LINKSET=0,REF=0,SLC=0,BPOS=0,BLINK=0,CELLSTR=0,VPI=1,VCI=8,OPTIONS=0x0002;
MTP_LINK:LINK=1,IFTYPE=ATM,LINKSET=1,REF=0,SLC=0,BPOS=0,BLINK=1,CELLSTR=1,VPI=1,VCI=8,OPTIONS=0x0002;
MTP_LINK:LINK=2,IFTYPE=ATM,LINKSET=0,REF=1,SLC=1,BPOS=0,BLINK=2,CELLSTR=2,VPI=1,VCI=8,OPTIONS=0x0002;
MTP_LINK:LINK=3,IFTYPE=ATM,LINKSET=1,REF=1,SLC=1,BPOS=0,BLINK=3,CELLSTR=3,VPI=1,VCI=8,OPTIONS=0x0002;
*
*   MTP route Configuration :
*   MTP_ROUTE:[NC=NC0],C7RT=,DPC=,LS1=[,UPMASK=0x0028][,OPTIONS=0][,LS2=0][,LABEL=];
MTP_ROUTE:NC=NC0,C7RT=0,DPC=3,LS1=0,UPMASK=0x0008;
MTP_ROUTE:NC=NC1,C7RT=1,DPC=3,LS1=1,UPMASK=0x0008;
*
*
* User part configuration….
*
```

7.14 Simultaneous MAP / INAP / IS41 Operations

The SIU supports the ability to run MAP, IS41, or INAP on the system at the same time. To achieve this, the outgoing dialog ID ranges are automatically divided equally between the configured protocols. The application should be configured to use matching ranges. The base dialog IDs will be allocated in sequence, starting with MAP, then INAP, and IS41.

- The base dialog ID for the first protocol will always be zero.
- The base dialog ID for the second protocol will be the total number of TCAP dialogs divided by the number of configured protocols (1 to 3).
- The base dialog ID for the third protocol will be 2x the total number of TCAP dialogs divided by the number of configured protocols (1 to 3).

The table below shows the distribution of dialog IDs and base dialog IDs, assuming that the maximum numbers of supported TCAP dialogs (32768) are configured.

	Outgoing Dialogs			**Base Outgoing Dialog ID**		
	MAP	**INAP**	**IS41**	**MAP**	**INAP**	**IS41**
MAP	32768	-	-	0	-	-
INAP	-	32768	-	-	0	-
IS41	-	-	32768	-	-	0

MAP & INAP	16384	16384	-	0	16384	-
MAP & IS41	16384	-	16384	0	-	0
INAP & IS41	-	16384	16384	-	0	16384
MAP & INAP & IS41	10922	10922	10922	0	10922	21844

7.15 GTT Configuration

Global Title Translation (GTT) is a process used to add or modify information in Global Titles to enable messages to be routed onwards. This may take the form of adding a Point Code or Subsystem Number or modifying the Global Title Address Information.

Typically, GTT examines the Global Title of a Called Party Address and compares it to the rules configured. If the Global Title and Global Title Address Information match, then the translation is performed. The message is then routed accordingly as it passes down the SS7 Protocol stack.

GTT support allows for simple translation of GTAI digits from one number to another. GTT also supports translations using wildcard matching to identify blocks of numbers which require the same translation operation as well as more sophisticated translations which drop or insert blocks of numbers.

Global Title Translation is a function performed by SCCP.

GTT is performed in two stages. First, the 'match' stage identifies which digits should be matched and which should be ignored, through either single digit or variable length wildcards. The second stage defines the translation operation to be performed. The user can specify to keep the digits in the address being translated, replace them with specified digits, or drop that block of digits.

There are three components to a GTT rule when configured using the config.txt file:

- The Pattern component, which specifies the GT information which must be matched.
- The Address component, which specifies the Address information to use when translating.
- The GTT Rule component, which controls how the Address Global Title is used during the translation process. The GTT Rule can additionally specify a Backup Address which is used if the first cannot be routed to at that time.

7.15.1 Global Title Address Information

GTAI digits may be split up into logical sections using the "/" separator character. Each section will contain zero or more digits.

Each section in the Pattern defines a set of digits which must be matched. Valid digits are in the ranges "0-9", "a-d" and "f". Wild cards may be used where the value of the digits is not significant. The "?" character represents a single digit wildcard, and the "+" character indicates a variable-length wildcard. If no digits are supplied for a section, then the section has no effect on the matched digits. An empty section is used to mark the position in the GTAI digits where digits are inserted from the Address. Padding characters may be added to aid readability.

Each section in the GTT Rule Mask defines how the replacement operation is performed. Sections marked "K" identify that the section of the Called Address being translated should be kept. Sections marked "R" identify that the section of the Called Address being translated should be replaced with digits from the Address component referenced by the GTT Rule. GTT Rule sections should not be empty.

7.15.2 Examples

Example 1

- Match GTAI digits 09876543210.
- Remove the GTAI and add a PC (138) and SSN (8).

Component	PC	SSN	GTAI Digits
Input			09876543210
Pattern			09876543210
Address	138	8	-
Rule			R
Output	138	8	

```
*
* Specific Address to PC + SSN
* This example translates a received specific Global Title address (09876543210) into a
* combination of Point Code (138) and SSN (8).
*
*   SCCP GTT Pattern Configuration :
*   SCCP_GTT_PATTERN:[NC=NC0],GTPID=,AI=[,SPC=0][,SSN=0],GT=[,GTAI_PATTERN=];
SCCP_GTT_PATTERN:GTPID=11,AI=0x10,GT=0x001104,GTAI_PATTERN=09876543210;
*
*   SCCP GTT Address Configuration :
*   SCCP_GTT_ADDRESS:[NC=NC0],GTAID=,AI=[,GTT_SPC=0][,SSN=0],GT=[,GTAI_REPLACEMENT=];
SCCP_GTT_ADDRESS:GTAID=11,AI=0x03,GTT_SPC=138,SSN=8,GT=0;
*
*   SCCP GTT Translation Configuration :
*   SCCP_GTT:[NC=NC0],GTPID=,GTT_MASK=,PRI_GTAID=[,SEC_GTAID=][,GTTSRC=ANY][,BAK_DUAL=N][,OPTIONS=0];
SCCP_GTT:,GTPID=11,GTT_MASK=R,PRI_GTAID=11;
```

Example 2

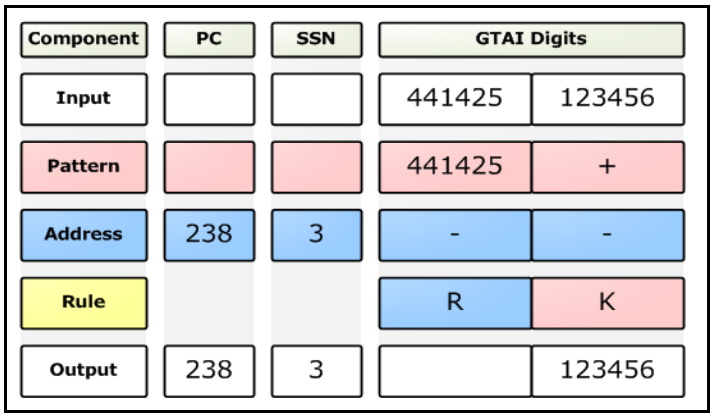
- Match a seven digit number starting "123", followed by any three digits, then "7".
- Change the first digits to "333". Keep the next three digits from the called-party address. Change the fourth digit to "4". Add a PC (11).

Component	PC	SSN	GTAI Digits		
Input			123	456	7
Pattern			123	???	7
Address	11		333	---	4
Rule			R	K	R
Output	11		333	456	4

```
*
*   Match a 7 digit number starting "123", followed by any three digits, then "7".
*   change the first digits to "333" keep the next three digits from the called-party
*   address and change the fourth digit to "4", and add a PC (11).
*
*
*   SCCP GTT Pattern Configuration :
*   SCCP_GTT_PATTERN:[NC=NC0],GTPID=,AI=[,SPC=0][,SSN=0],GT=[,GTAI_PATTERN=];
SCCP_GTT_PATTERN:GTPID=6,AI=0x10,GT=0x001104,GTAI_PATTERN=123/???/7;
*
*   SCCP GTT Address Configuration :
*   SCCP_GTT_ADDRESS:[NC=NC0],GTAID=,AI=[,GTT_SPC=0][,SSN=0],GT=[,GTAI_REPLACEMENT=];
SCCP_GTT_ADDRESS:GTAID=2,AI=0x11,GTT_SPC=11,GT=0x001104,GTAI_REPLACEMENT=333/---/4;
*
*   SCCP GTT Translation Configuration :
*   SCCP_GTT:[NC=NC0],GTPID=,GTT_MASK=,PRI_GTAID=[,SEC_GTAID=];
SCCP_GTT:GTPID=6,GTT_MASK= R--/K--/R,PRI_GTAID=2;
```

Example 3

- Match "441425", followed by any digits.
- Remove the first six digits. Keep any following digits in the Input GTAI. Add a PC(238) & SSN (3).

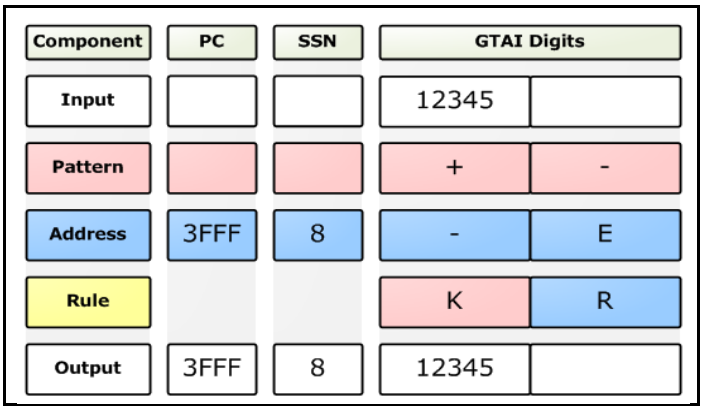


Component	PC	SSN	GTAI Digits	
Input			441425	123456
Pattern			441425	+
Address	238	3	-	-
Rule			R	K
Output	238	3		123456

```
A Matching Prefix to PC + SSN
This example translates any global title address matching a pattern consisting of a
prefix (441425) following by a suffix of any digits and any length into
a combination of Point Code (235) and SSN (3).
*
*
*   SCCP GTT Pattern Configuration :
*   SCCP_GTT_PATTERN:[NC=NC0],GTPID=,AI=[,SPC=0][,SSN=0],GT=[,GTAI_PATTERN=];
SCCP_GTT_PATTERN:GTPID=12,AI=0x10,GT=0x001104,GTAI_PATTERN=441425/+;
*
*   SCCP GTT Address Configuration :
*   SCCP_GTT_ADDRESS:[NC=NC0],GTAID=,AI=[,GTT_SPC=0][,SSN=0],GT=[,GTAI_REPLACEMENT=];
SCCP_GTT_ADDRESS:GTAID=12,AI=0x03,GTT_SPC=238,SSN=3,GT=0,GTAI_REPLACEMENT=-/-;
*
*   SCCP GTT Translation Configuration :
*   SCCP_GTT:[NC=NC0],GTPID=,GTT_MASK=,PRI_GTAID=[,SEC_GTAID=];
SCCP_GTT:GTPID=12,GTT_MASK= R/K,PRI_GTAID=12;
```

Example 4

- Match a GT with any GTAI Digits.
- Keep any digits which are present and add a PC and SSN.



Component	PC	SSN	GTAI Digits	
Input			12345	
Pattern			+	-
Address	3FFF	8	-	E
Rule			K	R
Output	3FFF	8	12345	

```
*   Adding a PC + SSN to any GTAI
*   This example matches any GTAI Digits and adds a Point Code and SSN, retaining any GTAI digits.
*
*    SCCP GTT Pattern Configuration :
*    SCCP_GTT_PATTERN:[NC=NC0],GTPID=,AI=[,SPC=0][,SSN=0],GT=[,GTAI_PATTERN=];
SCCP_GTT_PATTERN:GTPID=1,AI=0x10,SSN=0x03,GT=0x001204,GTAI_PATTERN=+/-;
*
*    SCCP GTT Address Configuration :
*    SCCP_GTT_ADDRESS:[NC=NC0],GTAID=,AI=[,GTT_SPC=0][,SSN=0],GT=[,GTAI_REPLACEMENT=];
SCCP_GTT_ADDRESS:GTAID=1,AI=0x53,GTT_SPC=0x3fff,SSN=0x08,GT=0x001204,GTAI_REPLACEMENT=-/e;
*
*    SCCP GTT Translation Configuration :
*    SCCP_GTT:[NC=NC0],GTPID=,GTT_MASK=,PRI_GTAID=[,SEC_GTAID=];
SCCP_GTT:GTPID=1,GTT_MASK=K/R,PRI_GTAID=1;
```

7.16 HSL Signaling

The Signaling Server supports both structured (framed) HSL links in accordance with ITU Q.703, Annex A.

HSL links can be configured on systems employing Dialogic® DSI SS7MD Network Interface Boards, which support up to 4 HSL links per board or 8 HSL links per unit.

7.16.1 MTP_LINK - IFTYPE

The MTP_LINK command supports the parameter, IFTYPE, that identifies the interface type for signaling links.

For HSL the interface mode should be set to one of the following values:

Interface_mode	Description
E1_FRAMED	Framed 31 timeslot E1 operation
T1_FRAMED	Framed 24 timeslot T1 operation
PCM	Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling)

The interface_mode value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.

7.16.2 MTP_LINK - OPTIONS

Bit number	Description
10 & 11	Set both to zero for E1_FRAMED and T1_FRAMED operation. HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link.
12	Sequence number length. Set to 1 the HSL signaling link will use a 12bit sequence number. If set to 0, the HSL signaling link will use a 7bit sequence number.

7.16.3 MTP_LINK - TS

For HSL links, the TS parameter should be set to 0xff to indicate that the link is attached to an LIU configured with the LIU_CONFIG command.

HSL signaling links may not use timeslots already configured for signaling or data. TDM links may not use timeslots already configured for HSL or data.

7.17 Monitoring

The SIU provides the ability to act either as a high-performance protocol monitor or to act in a mixed mode, both terminating as well as monitoring Signaling links.

Monitoring may be configure by specifying the board to be used for monitoring using the SS7_BOARD config.txt command, the LIU using the LIU_CONFIG command and the specific monitoring link using the LIU_CONFIG command.

A typical monitoring application requires that the monitoring E1/T1 must be configured as “high-impedance” to avoid corruption of the signal on the line. High-impedance can be configured on the LIU by setting the liu_type parameter to 6 for “E1 high impedance” or 7 for “T1 high impedance”.

A monitor link can be configured using the MONITOR_LINK command in the config.txt file. The following example demonstrates monitoring of signaling on timeslot 16 on a PCM where both the send and receive are transmitted to an application with module id 0x0d on host 0.

```
*MONITOR_LINK <MLINK> <IFTYPE> <BPOS> <BLINK> <BPOS2> <STREAM> <TS> <USER_ID> <USER_HOST> <OPTIONS>
MONITOR_LINK0TDM0       10 0  16   0x0d       0       0x0000
MONITOR_LINK1TDM02 0    1    16   0x0d       0          0x0000
```

Once configured, whenever a frame is received, it is reported to the user's application on the host as an API_MSG_RX_IND message or API_MSG_RX_INDT if timestamps are configured by setting bit 0 of the flags field to 1.

The following are examples of messages without timestamping enabled:

```
S7L:I0000 M t8f01 i0000 f00 d0d s00 pffff0103
S7L:I0000 M t8f01 i0000 f00 d0d s00 pffff0103
```

The following are examples of messages with timestamping enabled:

```
S7L:I0000 M t8f0f i0000 f00 d0d s00 pffff01037caa8ec4e90f2abf
S7L:I0000 M t8f0f i0000 f00 d0d s00 pffff01037caa8ec4c3976bbf
```

During operation, the user may also read (and optionally reset) various statistics on a per-link basis using the MSMLP MMI command and view status on the links using the STMLP command.